No: 2024-2256

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

LARRY GOLDEN
Plaintiff-Appellant

v.

The United States
Defendant-Appellee

ON APPEAL FROM THE UNITED STATES COURT OF FEDERAL CLAIMS IN GOLDEN v. THE UNITED STATES [DEFENSE THREAT REDUCTION AGENCY] IN 1:2023cv00811-EGB; JUDGE ERIC BRUGGINK

PLAINTIFF-APPELLATE'S MOTION FOR ORAL ARGUMENT

LARRY GOLDEN, *Pro Se*
740 Woodruff Rd., #1102
Greenville, S.C. 29607
(864-288-5605)
Atpg-tech@charter.net

January 18, 2025

CONTENTS

Page

APPELLANT WILL ARGUE EMINENT DOMAIN AND TAKING PATENT LICENSES 1

Standard for Review 1
Scope of Section 1498(a) 2
28 U.S.C. § 1498(a) is "its own independent cause of action" 3

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE WAS FIRST REQUESTED IN THE DHS SBInet INITIATIVE 4

Technology 5

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE COVERED IN APPELLANT'S PATENTS 6

Golden's Patents' Written Support for His Claimed Anti-Terrorism Inventions 6

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE *COLLECTIVELY* COVERED IN APPELLANT'S PATENT CLAIMS 7

Claims 1-12 of Golden's Patent No. 9,589,439 8

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE *INDIVIDUALLY* COVERED IN APPELLANT'S PATENT CLAIMS 10

Claim 23 of Golden's Patent No. 9,589,439 10
Claims 1-10 of Golden's Patent No. 10,984,619 11

Claim 1 of Golden's Patent No. 11,645,898 12

APPELLANT WILL ARGUE THE DEVICES DEVELOPED IN THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRAATAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE FOR THE GOVERNMENT 13

"For the Government" 13
"Authorization or Consent" 14

APPELLANT WILL ARGUE TEN FEDERAL JUDGES WHO HAS REVIEWED GOLDEN'S PATENTED INVENTIONS COMBINATIONS ALL AGREE THE GOVERNMENT IS THE "SINGLE ENTITY' WHO ALLEGEDLY INFRINGED GOLDEN'S PATENTS UNDER 28 U.S.C. § 1498(a) 16

The United States Court of Federal Claims in *Golden v. US*, Case No. 13-307C; determined Direct Infringement by or for the Government, arises when there's a combined Mobile Device; CPU; CBRNE Detector/Sensor; and/or Unmanned Aerial Vehicle 17
Since Judge Bruggink's Decision in *Golden v. Us* Case No. 13-307C; Nine Federal Judges Infer the United States Directly Infringed Golden's Patented Inventions Combinations 19

APPELLANTWILLARGUE THE GOVERNMENT ADMITS ITS OWN LIABILITY 20

Google Tensor "CPU" 20
DHS S&T "*Cell-All*" 21
DoD DTRAATAK—CBRNE Plugin Sensors 22
DoD "JPEO-CBRND" 23
The Fifth Amendment of the United States Constitution 24
U.S. Supreme Court 24

APPELLANTWILLARGUE THE GOVERNMENT'S WORSENING OF EARLIER CONDITIONS 25

CONCLUSION 29

28 U.S.C. § 1498(a) is "its own independent cause of action" 29
The Fifth Amendment of the United States Constitution 30
U.S. Supreme Court 30

APPELLANT WILL ARGUE EMINENT DOMAIN AND TAKING PATENT LICENSES

Standard for Review

On June 25, 1910, Congress passed "An Act to provide additional protection for owners of patents of the United States" (1910 Act), stating in pertinent part:

> "[t]hat whenever an invention described in and covered by a patent of the United States shall hereafter be used by the United States without license of the owner thereof or lawful right to use the same, such owner may recover reasonable compensation for such use by suit in the Court of Claims."

Dubbed the "Government Use Statute," the 1910 Act created a means for patent owners to obtain money damages for the government's use of patented inventions while at the same time not restricting the government's use. *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1283 (Fed. Cir. 1988) ("The patentee takes his patent from the United States subject to the government's eminent domain rights to obtain what it needs from manufacturers and to use the same."), abrogated on other grounds by *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391–94 (2006).

Congress styled the 1910 Act under the theory of eminent domain, as the government's taking of a license to use a patented invention would be for the benefit of the public. *Crozier*, 224 U.S. at 305 ("[I]n view of the public nature of the subjects with which the patents in question are concerned and the undoubted authority of the United States as to such subjects to exert the power of eminent domain, the statute, looking at the substance of things, provides for the appropriation of a license to use the invention, the appropriation thus made being sanctioned by the means of compensation for which the statute provides.").

As stated in *Calhoun v. United States*, "when a patented device or invention is made or used by or for the United States, [the government] *ipso facto* takes by eminent domain a compulsory compensable license in the patent; the patentee obtains his Fifth Amendment just compensation for that taking through his action [in the USCFC] under § 1498." 453 F.2d 1385, 1391 (Ct. Cl. 1972). The takings clause of the Fifth Amendment states that "private property [shall not] be taken for public use, without just compensation." [U.S. Const. amend. V.]

Congress passed the 1918 version of the "Government Use Statute" that clarified the government's assumption of liability for a contractor's unlawful use or manufacture of a patented

invention and limited a plaintiff's sole remedy to monetary compensation. Act of July 1, 1918, Pub. L. No. 65-182, 40 Stat. 704, 705; *Zoltek V*, 672 F.3d at 1316.

Section 1498(a) took its present form in 1949, and retains the bedrock principles established in 1910 and 1918 of (1) defining the government's unlawful use or manufacture of patented articles as a Fifth Amendment taking of a license to use a patented invention, (2) providing government contractor immunity from patent infringement litigation, and (3) limiting available remedies to monetary damages. Act of May 24, 1949, Pub. L. No. 81-72, § 87, 63 Stat. 89, 102. Section 1498(a) provides in pertinent part:

> "[w]henever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture . . . For the purposes of this section, the use or manufacture of an invention described in and covered by a patent of the United States by a contractor, a subcontractor, or any person, firm, or corporation for the Government and with the authorization or consent of the Government, shall be construed as use or manufacture for the United States. 28 U.S.C. § 1498(a)."

Scope of Section 1498(a)

As § 1498(a) infringement actions are grounded in eminent domain and not defined by statute, the scope of what constitutes the unlawful taking of a license to use a patent is a creature of case law. As such, the basis for the USCFC's jurisdiction over infringement actions must be linked to the government's taking of a patent license through its "use or manufacture" of the patented invention "without license of the owner thereof or lawful right." *Decca Ltd. v. United States*, 640 F.2d 1156, 1166–67 (Ct. Cl. 1980). [***Exhibit A***]

In contrast, the Patent Act—the statutory basis that governs the processes for issuing and enforcing patents before the United States Patent and Trademark Office (USPTO) and the district courts—defines patent infringement as a statutory tort in 35 U.S.C. § 271. *See*, 35 U.S.C. § 271(a)–(c), (e)–(g); *see* also *Decca*, 640 F.2d at 1166 ("Because section 1498 authorizes the Government to take a license in any United States patent, the Government is never 'guilty' of 'direct infringement' of a patent insofar as 'direct infringement' connotes tortious or wrongful conduct."). Before the enactment of § 1498, the government would routinely contest the Court of Claims' jurisdiction to hear patent actions, as such actions traditionally sound in tort. Sean M. O'Connor, Taking, Tort, or Crown Right?—*The Confused Early History of Government Patent*

Policy, 12 J. Marshall Rev. Intell. Prop. L. 145, 165–67 (2012). The Supreme Court also heard some congressional reference cases on the government's patent infringement. *See, e.g., James v. Campbell*, 104 U.S. 356, 357 (1882).

In *Horne v. Department of Agriculture*, the Court held that the Takings Clause imposes a "categorical duty" on the government to pay just compensation whether it takes personal or real property. Chief Justice Roberts, writing for the Court, noted the long history of private property being secured against uncompensated takings by the government, beginning with the Magna Carta some 800 years ago. In further support, Roberts cited a Supreme Court opinion from the late nineteenth century:

> "Nothing in this history suggests that personal property was any less protected against physical appropriation than real property. As this Court summed up in *James v. Campbell*, 104 U.S. 356,358 (1882), a case concerning the alleged appropriation of a patent by the Government":
>
> > *"[A patent] confers upon the patentee an exclusive property in the patented invention which cannot be appropriated or used by the government itself, without just compensation, any more than it can appropriate or use without compensation land which has been patented to a private purchaser."*

Section 271(a) of the Patent Act provides: "whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent." *In contrast, § 1498(a) only references patented inventions "used or manufactured by or for the United States" as potentially infringing acts.*

28 U.S.C. § 1498(a) is "its own independent cause of action"

In *Zoltek III*, the Federal Circuit further narrowed§ 1498 by holding that direct infringement under§ 1498(a) with respect to the United States' use or manufacture of a patented invention was predicated on§ 271(a) of the Patent Act. See *Zoltek Corp. v. United States* (*Zoltek III*), 442 F.3d 1345, 1350 (Fed. Cir. 2006), abrogated by *Zoltek V*, 672 F.3d 1309, 1322–23 (Fed. Cir. 2012) (en bane); *see* also *NTP, Inc. v. Research in Motion, Ltd*., 418 F.3d 1282, 1316 (Fed. Cir. 2005) ("[D]irect infringement under section 271(a) is a necessary predicate for government liability under section 1498."); *Motorola, Inc. v. United States*, 729 F.2d 765, 768 n.3 (Fed. Cir. 1984).

However, in the 2012 *en bane* decision *Zoltek V*, the Federal Circuit abrogated *Zoltek III*, holding that establishing conduct falling within the definition of direct infringement codified in 35 U.S.C. § 271(a) is not a predicate to finding infringement under § 1498(a). Instead, the court concluded that the scope of § 1498(a) is "linked to the scope of the patent holder's rights as granted by the patent grant in title 35 U.S.C. section 154(a)(1)." *Zoltek V*, 672 F.3d at 1323. In contrast to the statutory definitions of infringement in § 271, § 154(a)(1) defines the patent grant issued by the USPTO as:

> "[T]he right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States, and, if the invention is a process, . . . the right to exclude others from using, offering for sale or selling throughout the United States, products made by that process, referring to the specification for the particulars thereof. 35 U.S.C. § 154(a)(1)."

In *Zoltek V*, the appellate court emphasized that § 1498(a) is "its own independent cause of action" with three elements to trigger government liability: (1) the invention must be claimed in a patent; (2) it must be "used or manufactured by or for the United States," meaning each limitation of the claims must be present in the accused product or process; and (3) the "use or manufacture" of the patented invention must be done without license or lawful right—i.e., "use of an invention that, if done by a private party, would directly infringe the patent." 672 F.3d at 1321, 1323.

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE WAS FIRST REQUESTED IN THE DHS SBInet INITIATIVE

> SBInet was a program initiated in 2006 for a new integrated system of personnel, infrastructure, technology, and rapid response to secure the northern and southern land borders of the United States. It was a part of Secure Border Initiative (SBI), an overarching program of the United States Department of Homeland Security (DHS) to organize the four operating components of border security: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement, United States Citizenship and Immigration Services, and the United States Coast Guard. DHS announced the program's cancelation on Jan. 14, 2011.
>
> SBInet replaced two former programs, America's Shield Initiative and the Integrated Surveillance Intelligence System. Both of these programs had similar goals, but were scrapped due to mismanagement and failure of equipment. To avoid such problems, DHS decided to have development of SBinet managed by a single

private contractor. Boeing, holding the primary contract, has subcontracted many portions of the design, development, implementation, and maintenance of the program, with Boeing handling the majority of the management aspects.

Boeing was required to design, develop, test, integrate, deploy, document and maintain the optimum mix of personnel, technology, infrastructure, and response capability to defend 6,000 miles of border. Boeing was required to manage every aspect of the implementation of SBInet; their job even includes less intuitive tasks, such as recommending new paradigms for the way Border Patrol Agents operate, training maintenance personnel to repair their products, and guiding construction of facilities to house additional CBP offices required for SBInet. Additionally, Boeing was required to integrate their program into previously existing infrastructure and equipment systems wherever possible.

Border patrol agents began using the system in December 2007, and the system was officially accepted by DHS in February 2008. Boeing was awarded further contracts to upgrade software and hardware, which it expected to have done by the end of 2008.

Technology

Tower system: Towers were meant to be set up along the border, with varying surveillance and communications equipment depending on the climate, terrain, population density, and other factors. Towers were slated to include radar, long-range cameras, broadband wireless access points, thermal imaging capabilities, and motion detectors. SBInet was meant to also include some ground sensors for seismic detection as well.

Command centers: All of the information received by sensors were meant to go to command centers, where a "common operating picture" would have been compiled by CBP and shared with other agencies. The common operating picture would have appeared on computer screens as a geospatial map, where border entries are tracked in real time. Command center personnel were supposed to be able to click on a given entry, view the entry, and assess the threat using the long-range cameras on the towers. They will then dispatch Border Patrol agents accordingly.

Border Patrol response: Border Patrol agents were meant to carry PDAs with GPS capabilities, to allow the command center to track the location of agents interdicting illegal entries and watch the encounter in real time on the common operating picture. Additionally, the PDAs were supposed to have advanced finger print identification technology, to allow Border Patrol agents to identify an individual at the interdiction site immediately and the ability to view and control tower cameras from their PDA. In addition, Border Patrol agents will be given laptops in the patrol car that will provide them the information necessary to effectively and safely approach a given threat. ***[Specifics for the DHS S&T Cell-All initiative, and the DoD DTRA iTAK, ATAK & WinTAK CBRNE initiatives]***

Airborne sensors: Airborne sensors on unmanned aerial vehicles (UAVs) were meant to fill in gaps in the "virtual fence" in remote areas where building and maintaining towers is impractical. Boeing may employ a small UAV that a lone person can launch called the Skylark, made by Elbit Systems. ***[Specifics for the***

DHS S&T Cell-All initiative; the DoD DTRA iTAK, ATAK & WinTAK CBRNE initiatives; and, the DoD JPEO-CBRND initiative]

Construction strategy: The towers that will initially be placed in the pilot section will be mobile, so that they can be moved around to discover optimal placement. Once the optimal placement is determined, they will be replaced with permanent towers, and the mobile towers will be reused to begin construction on the next section of SBInet in a similar manner. At completion, Boeing estimates that it will use approximately 1,800 towers to create its "virtual fence" along the borders.

The fate of SBInet had been in question since DHS Secretary Janet Napolitano ordered an assessment of the project in January 2010 and in March 2010 froze additional funding for anything beyond already begun initial deployments. On Jan. 14, 2011, DHS said it would redirect funding originally intended for SBInet—including fiscal 2011 SBInet funds—to the new border security technology effort. [***Exhibit B***]

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE COVERED IN APPELLANT'S PATENTS

Golden's Patents' Written Support for His Claimed Anti-Terrorism Inventions

The present invention comprehends a chemical/biological/radiological/ nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. [***Exhibit C***]

The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, United Parcel Services™ (UPS™), Federal Express™ (FedEx™), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and utility vehicles;

the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels;

the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-

on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to;

the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop personal computers (PCs), notebook personal computers (PCs), laptops, satellite cell phones, cell phones, Universal Mobile Telecommunications System (UMTS) phones, personal digital assistants (PDAs), liquid crystal display (LCD) monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds;

the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS), Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS);

the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature;

the products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel.

The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE *COLLECTIVELY* COVERED IN APPELLANT'S PATENT CLAIMS

Claims 1-12 of Golden's Patent No. 9,589,439

1. A multi sensor detection system capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities vulnerable to terrorist activity that can be integrated with and interconnected to watchtowers to form a network, comprising:

at least one of an integrated watchtower, a fixed watchtower, a surveillance watchtower, a watchtower capable of scanning, a watchtower capable of monitoring, a watchtower equipped with sensors or a watchtower interconnected to a central monitoring terminal for sending signals thereto and receiving signals therefrom;

wherein the at least one watchtower is equipped with a remote video surveillance camera that provides at least one night vision means of surveillance or an infrared human detection means of surveillance capability and is integrated into a watchtower's remotely controlled system that can monitor, detect, track, and identify humans;

a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop personal computer (PC), a notebook personal computer (PC), a laptop, a satellite phone, a smart phone, a cell phone, a Universal Mobile Telecommunications System (UMTS) phone, a personal digital assistant (PDA), a liquid crystal display (LCD) monitor, a satellite, or a handheld, interconnected to a monitoring equipment for sending signals thereto and receiving signals therefrom;

a communication method of at least one of a Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), or central processing unit (CPU), used to interconnect the communication device to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a plurality of sensors for detecting or sensing humans that is at least one of a chemical human sensor, biological human sensor, radiological human sensor, infrared human detector, motion human detector, or image human detector, interconnected to or disposed within the multi-sensor detection system for sending signals thereto and receiving signals therefrom;

a mobile multi-sensor detection device that is at least one of a ground surveillance sensor, a surveillance radar sensor, a surveillance camera, or a stand-alone surveillance scanner, that is mounted in, on, or upon at least one of a car, a truck, a camper, a bus, a van, an unmanned aerial vehicle (UAV), an unmanned ground vehicle (UGV), or a utility vehicle, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a hand-held multi-sensor detection device that is capable of at least one of thermal imaging or infrared imaging for monitoring, detecting, tracking and identifying humans, that is controlled or operated by at least one authorized person who is an owner, pilot, conductor, captain, drivers of vehicles identified as high

security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, or monitoring site and terminal personnel, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, wherein the authorized person manually initiates the signal to the monitoring equipment to alert upon the monitoring, detecting, tracking and identifying of the human;

whereupon, detection by the mobile multi-sensor detection device causes an automatic signal transmission to be sent to, or received from, any products in product grouping categories of storage and transportation, sensors, detector case; modified and adapted, monitoring and communication devices, communication methods, biometrics;

whereupon, detection of an unauthorized vehicle, an unauthorized driver or operator of a vehicle or mobile unit, a signal is sent from the communication device to the vehicle or mobile unit to stop, stall or slowdown the vehicle;

wherein, a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop PC, a notebook PC, a laptop, a satellite phone, a smart phone, a cell phone, a UMTS phone, a PDA, a LCD monitor, a satellite, or a handheld, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, comprising a lock disabling mechanism that is able to engage (lock), and disengage (unlock) and disable (make unavailable) after a specific number of tries.

2. The multi sensor detection system of claim 1, capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities, further includes the identifying, monitoring, and detecting of terrorist, that is at least one of an illegal, radical, fanatic, activist, revolutionist or rebel.

3. The multi-sensor detection system of claim 1, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

4. The multi-sensor detection system of claim 1, further includes a navigation system adapted for communication with at least one of the surveillance watchtowers.

5. The multi-sensor detection system of claim 1, capable of forming a wired or wireless sensor network.

6. The multi-sensor detection system of claim 1, capable of forming a mesh network for redundancy.

7. The multi-sensor detection system of claim 1, capable of transmitting identification data, location data, power source data, and sensor data.

8. The multi-sensor detection system of claim 1, capable of being embedded into; placed in, on, or adjacent to at least one of the products in the product grouping categories or an area targeted for monitoring.

9. The multi-sensor detection system of claim 1, capable of sending signals thereto and receiving signals therefrom to engage (lock), disengage (unlock) and disable (make unavailable) a lock after a specific number of tries that is interconnected to the multi sensor detection system or monitoring equipment.
10. The multi-sensor detection system of claim 1, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.
11. The multi-sensor detection system of claim 1, interconnected with a camera to view the environment in real-time or to store the data for transmission and review at a later time.
12. The multi-sensor detection system of claim 1, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE *INDIVIDUALLY* COVERED IN APPELLANT'S PATENT CLAIMS

Claim 23 of Golden's Patent No. 9,589,439

23. A cell phone comprising:

a central processing unit (CPU) for executing and carrying out the instructions of a computer program;

a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and

whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;

wherein at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection is capable of

signal communication with the transmitter or the receiver;

wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and

whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.

Claims 1-10 of Golden's Patent No. 10,984,619

1. A communication device that is at least a personal computer (PC), a cellphone, a smartphone, a laptop, or a handheld scanner, comprising at least a central processing unit (CPU), capable of:

processing instructions to lock, unlock, or disable the lock of the communication device;

processing instructions to activate a lock, unlock, or disabling lock means by engaging a vehicle with a two-way communication key-fob;

processing instructions to activate a start, stall, stop, or disabling means by engaging a vehicle's ignition system;

processing instructions to activate a lock, unlock, or disabling lock means; a start, stall, stop, or disabling vehicle means by engaging the operational systems of the unmanned aerial vehicle;

processing instructions to authenticate or identify a user by at least one of biometric fingerprint recognition, biometric facial recognition, biometric iris recognition, or biometric retina recognition;

processing instructions to scan a senor or tag using the short-range wireless technology of radio frequency near-field communication (NFC);

processing instructions to monitor or detect at least one of a chemical sensor, a biological sensor, a motion sensor, a biometric sensor, a signature sensor, or a human sensor;

processing instructions to monitor or detect for at least one of chemical agent, biological agent, radiological agent, nuclear agent, or explosive agent, weapons of mass destruction (WMDs);

processing instructions received through at least one of a Bluetooth, a Wi-Fi, a satellite, a global positioning system (GPS), or a cellular transmission;

processing instructions to connect the communication device to the internet or internet-of-things (IoTs) platform to sync, to at least one of a building's computer or security system, a vehicle's computer or security system, a lock, a detection device, or another communication device; and,

whereupon, the communication device is capable of processing instructions for operational and functional execution, and is capable of providing feedback of the execution, and storing the feedback into memory.

2. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of processing operational instructions for at least a personal computer (PC), a cellphone, a smartphone, a laptop, or a handheld

scanner.

3. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal to lock, unlock, or disable the lock of the communication device.

4. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal ofat least fingerprint recognition, facial recognition, iris recognition, or retina recognition.

5. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of at least short-range wireless radio frequency near-field communication (NFC).

6. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal from at least chemical sensor, biological sensor, motion sensor, biometric sensor, signature sensor, or human sensor.

7. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal from at least one of chemical, biological, radiological, nuclear, or explosives detection.

8. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal through at least a Bluetooth, a Wi-Fi, a satellite, a cellular, or GPS connection.

9. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of the communication device connection to the internet or internet-of-things (IoTs) platform to sync at least a building's computer or security system, a vehicle's computer or security system, a lock, a detection device, or another communication device.

10. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of the operational and functional execution of instructions; capable of providing feedback of the execution; and, capable of storing the feedback into memory.

Claim 1 of Golden's Patent No. 11,645,898

1. A pre-programmed stall, stop, vehicle slow-down system, that comprises at least one central processing unit (CPU), capable of:

processing instructions to stall, stop, or slow-down a vehicle when the vehicle receives a signal from at least one of a personal computer (PC), a cellphone, a smartphone, a laptop, a tablet, a PDA, or a handheld;

processing instructions to stall, stop, or slow-down a vehicle when the vehicle receives a signal from at least one of cellular, satellite, or radio-frequency (RF);

processing instructions to stall, stop, or slow-down a vehicle when the vehicle is experiencing unintended acceleration;

processing instructions to stall, stop, or slow-down a vehicle when the vehicle is experiencing lane departure;

processing instructions to stall, stop, or slow-down a vehicle when a collision or crash is detected;

processing instructions to stall, stop, or slow-down a vehicle when the vehicle has been reported as stolen;

processing instructions to stall, stop, or slow-down a vehicle when the vehicle has moved outside a pre-programmed designated perimeter;

processing instructions to stall, stop, or slow-down a vehicle when at least one of a chemical hazard, a biological hazard, a radiological hazard; a nuclear hazard; or explosives have been detected;

processing instructions to stall, stop, or slow-down a vehicle when the vehicle is at least a driverless vehicle; a self-drive vehicle; an autonomous vehicle; a human controlled vehicle; a manned or unmanned convoy vehicle, or a manned or unmanned aerial, land, or sea vehicle; and,

Wherein, when the central processing unit (CPU) processes instructions to stall, stop, or slow-down a vehicle, a distress signal is sent to at least one of a monitoring site, a control center, or is recorded for storage.

APPELLANT WILL ARGUE THE DEVICES DEVELOPED IN THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA ATAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE ARE FOR THE GOVERNMENT

"For the Government"

In *Advanced Software Design Corp. v. Federal Reserve Bank of St. Louis*, the Federal Circuit interpreted the term "for the government" to mean that the government derives a benefit from the use or manufacture of the patented technology. 583 F.3d 1371, 1376–77 (Fed. Cir. 2009). For example, the patented technology itself must be used "in furtherance and fulfillment of a stated Government policy," which would serve the government's interest, for the government's benefit. *IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359, 1362 (Fed. Cir. 2014) (quoting *Madey v. Duke Univ.*, 413 F. Supp. 2d 601, 607 (M.D.N.C. 2006)).

In light of the allegations that the inventions disclosed in patents '189, '439, '287, '619, and '898 were designed to prevent terrorist activity, it is plausible that the government agencies and private entities manufactured the infringing devices for the benefit of the DHS & DoD to promote national security. *see, e.g., Hughes Aircraft Co.*, 534 F.2d at 898 (finding that the government's participation in a satellite program was "for the Government," because the program was vital to the military defense and security of the United States).

On September 17, 2015, the Federal Circuit affirmed the dismissal under 28 U.S.C. § 1498(a) of a patentee's claims for indirect patent infringement against government contractors where the only alleged directed infringement was the Government's purported use of the

patented invention. *Astornet Technologies Inc. v. BAE Systems, Inc.*, No. 14-1854 (Fed. Cir. Sept. 17, 2015). The decision is another in a line of recent Federal Circuit decisions reaffirming that government contractors enjoy broad immunity from traditional patent infringement liability under § 1498.

Therefore, ten judges; one from the Court of Federal Claims, six from the Federal Circuit and three from the Northern District of California, acknowledged the "U.S. Government", the single entity under 28 USC § 1498 for direct infringement, is more likely than not, the direct infringer because the element-by-element requirement is only satisfied under 28 USC § 1498 when Golden's entire patented inventions combinations are made and are "suitable for use".

"Authorization or Consent"

The government's authorization of or consent to a contractor's infringing activity may be express or implied. *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986); *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976).

Appellant's complaints allege sufficient facts to plausibly establish that the use of the accused devices was "with the authorization or consent of the Government." Authorization or consent can be implied from the circumstances, "e.g., by contracting officer instructions, [or] specifications or drawings which impliedly sanction and necessitate infringement." *Hughes Aircraft Co.*, 534 F.2d at 901. For example, in *TVI Energy Corp.*, the United States Court of Appeals for the Federal Circuit held that the Government impliedly sanctioned the use of a patented invention when it issued a solicitation that required bidders to submit for inspection, and perform live demonstrations of, the accused device. *See TVI Energy Corp.*,806 F.2d at 1060."

The Federal Acquisition Regulation (FAR) 52.227-1 contains an express grant of "authorization and consent" for contractors and subcontractors for the use and manufacture of any patented invention (1) embodied in the structure or composition of any article delivered to and accepted by the government related to a government contract; or (2) used in machinery, tools, or methods necessary for a contractor to comply with the specifications of a contract, or if such use is directed by a contracting officer's specific written instructions. 48 C.F.R. § 52.227-1; *see* also *Sevenson Envtl. Servs., Inc. v. Shaw Envtl., Inc.*, 477 F.3d.

In *Larson v. United States*, the Claims Court recognized that implied authorization "may be found under the following conditions: (1) the government expressly contracted for work to

meet certain specifications; (2) the specifications cannot be met without infringing on a patent; and (3) the government had some knowledge of the infringement." *Larson*, 26 Cl. Ct. at 370 (citing *Bereslavsky v. Esso Standard Oil Co.*, 175 F.2d 148, 150 (4th Cir. 1949); *Carrier Corp. v. United States*, 534 F.2d 244, 247–50 (Ct. Cl. 1976); *Hughes*, 534 F.2d at 897–901).

Example of implied authorization: Each of the three initiatives asserted in this case; the DHS S&T *Cell-All* initiative; the DOD DTRA iTAK, ATAK, and WinTAK CBRNE initiatives; and, the DOD JPEO-CBRND initiative, are all issued with an implied authorization for at least one of Golden's patented central processing units (CPUs) because the CPUs are considered the "brains" of the asserted devices and is responsible for carrying out the operational and functional instructions of the computer program: Without expressly requesting the central processing units (CPUs), here's how notice is given in the *Cell-All* solicitation:

> "Include all hardware, software and data deliverables" ... "Provide a brief summary of all deliverables proposed under this effort, including data, software, and reports consistent with the objectives of the work" ... "Include here a summary of any assertions to any technical data or computer software that will be developed or delivered under any resultant award" ... "Proposals submitted in response to this solicitation shall identify all technical data or computer software that the Offeror asserts will be furnished to the Government with restrictions on access, use, modification, reproduction, release, performance, display, or disclosure" ... "The Offeror asserts for itself, or the persons identified below, that the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose only the following technical data or computer software should be restricted:" ... "Identification of the technical data or computer software to be furnished with restrictions" ... "For computer software or computer software documentation, identify the software or documentation by specific name or module or item number" ... "Identify the asserted rights for the technical data or computer software" ... "For computer software, development refers to the development of the software. Indicate whether development was accomplished exclusively or partially at private expense" ... "The Offeror shall identify the technical data or computer software that are identical or substantially similar to technical data or computer software that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or subcontract" ... "The estimated cost of development for that technical data or computer software to be delivered with less than Unlimited Rights" ... "The contract number under which the data or software were" ... "The contract number under which, and the name and address of the organization to whom, the data or software were most recently delivered or will be delivered" ... "Identification of the expiration date for any limitations on the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose the data or software, when applicable" ... [DHS S&T (BAA) BAA07-10 CELL-ALL Ubiquitous Biological and Chemical Sensing; Published 10/30/2007: DHS request for "software" made in the Cell-All specifications]

APPELLANT WILL ARGUE TEN FEDERAL JUDGES WHO HAS REVIEWED GOLDEN'S PATENTED INVENTIONS COMBINATIONS ALL AGREE THE GOVERNMENT IS THE "SINGLE ENTITY' WHO ALLEGEDLY INFRINGED GOLDEN'S PATENTS UNDER28 U.S.C. § 1498(a)

Although, it was not the intention of the United States Judges to confirm the United States liability for direct infringement under 28 U.S.C. § 1498(a); they inadvertently confirmed the United States liability when the judges collectively agreed: "direct infringement occurs when the products that allegedly infringes Golden's patented inventions are combined to create a product(s) "suitable for use".

Under 28 USC § 1498, the patentee's "exclusive remedy for an alleged infringement by or for the Government, which means the Government is the 'single entity' for the purpose of direct infringement, is a suit against the United States in the Court of Federal Claims."

The statue serves two purposes: (i) it waives sovereign immunity to permit a patent owner to recover damages for direct infringement "by or for the United States" as the single entity, and (ii) it protects contractors from liability for patent infringement committed on behalf of the United States.

The courts emphasized that the remedy provided in § 1498 is the "exclusive remedy" available when the U.S. Government, as the single entity, directly infringes a patent. A recent trend of Federal Circuit decisions, including *IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359 (Fed. Cir. 2014) and *Zoltek Corp. v. United States*, 672 F.3d 1309 (Fed. Cir. 2012), holding that§ 1498 affords government contractors a wide scope of protection against liability for infringement.

In the words of the Federal Circuit, there is "no justification" for "expos[ing] a significant range of government contractors to direct liability (and possible injunctive remedies), namely, those [that may be] accused of indirect infringement of claims [that are] directly infringed by the government."

On September 17, 2015, the Federal Circuit affirmed the dismissal under 28 U.S.C. § 1498(a) of a patentee's claims for indirect patent infringement against government contractors where the only alleged directed infringement was the Government's purported use of the patented invention. *Astornet Technologies Inc. v. BAE Systems, Inc.*, No. 14-1854 (Fed. Cir. Sept. 17, 2015). The decision is another in a line of recent Federal Circuit decisions reaffirming that

government contractors enjoy broad immunity from traditional patent infringement liability under§ 1498.

Therefore, ten judges, one from the Court of Federal Claims [Judge Susan Braden], six from the Federal Circuit and three from the Northern District of California, acknowledged the "U.S. Government', the single entity under 28 USC § 1498 for direct infringement, is more likely than not, the direct infringer because the element-by-element requirement is only satisfied under 28 USC § 1498 when Golden's entire patented invention combinations are made and are "suitable for use".

The United States Court of Federal Claims in *Golden v. US*, Case No. 13-307C; determined Direct Infringement by or for the Government, arises when there's a combined Mobile Device; CPU; CBRNE Detector/Sensor; and/or Unmanned Aerial Vehicle

Judge Braden, in the United States Court of Federal Claims, *Golden v. United States*, Case No. 13-307C "Memorandum Opinion and Order Denying the Government's Motion to Dismiss, Dkt. 94, filed 11/30/16, fully described when a product is considered "manufactured" and is "suitable for use". In *FastShip, LLC v. United States*, the U.S. Court of Appeals for the Federal Circuit held that to be "manufactured" under 28 U.S.C. Section 1498, an accused product must include each claim limitation so it is "suitable for use'.

"The February 12, 2016 Amended complaint identifies over thirty devices that were developed or procured, as a result of Government solicitations, Government contracts. or National Science Foundation ("NSF") grants. 2/12/16 Am. Compl. at ¶¶ 68-127. The relevant devices. are: M-Lock; High-Power Electromagnetic System ("HPEMS"); Smartphone Microscope; Biophone; Smartphone Biosensor Cradle; iPhone Biodetector Smartphone; Pathtracker; the Center of Integrated Nanomechanical Systems ("COINS") Nano-Embedded Sensors; Smartphone-Based Rapid Diagnostic Tests; Lockheed Martin K-Max Unmanned Self-flying Helicopter; Boeing MH-6 Little Bird Helicopter; SIN-VAPOR I Smartphone System; Samsung Galaxy s6 Microscope Smartphone; VOCket System; Nett Warrior Smartphone System; Northrop Grumman X-47B UCAS I X-478 Control Display Unit; GammaPix; NFC Samsung Galaxy s6 Smartphone Sensor; Cell-All Synkera MikroKera Ultra; Biotouch System; iPhone Biodetector Smartphone; Navy Marine Corps Intranet; FLIR identiFINDER R300; AOptix Stratus MX Peripheral; MultiRae Pro Wireless Portable Multi Threat Radiation and Chemical Detector; PositiveID's M-BAND; PositiveID's Firefly DX; 1"x2" Detection Device

Samsung Galaxy s6 Smartphone; 2"x2" Detection Device Samsung Galaxy s6 Smartphone; NetS2 SmartShield G300 Radiation Detector Samsung Galaxy s6 Smartphone; NetS2 SmartShield G500 Radiation Detector Samsung Galaxy s6 Smartphone; and the Passport Systems Base Control Unit; Oshkosh Defense Autonomous Unmanned Ground Vehicle TerraMax; and the Variable NODE+Oxa. 2/72/76 Am. Compl. at, ¶¶ 68-127."

"The February 12, 2016 Amended Complaint's NFC claims also allege sufficient facts to plausibly establish that the use of the accused devices was "with the authorization or consent of the Government." Authorization or consent can be implied from the circumstances, "e.g., by contracting officer instructions, [or] specifications or drawings which impliedly sanction and necessitate infringement." *Hughes Aircraft Co.*, 534 F.2d at 901. For example, in *TVI Energy Corp.*, the United States Court of Appeals for the Federal Circuit held that the Government impliedly sanctioned the use of a patented invention when it issued a solicitation that required bidders to submit for inspection, and perform live demonstrations of, the accused device. *See TVI Energy Corp.,806 F.2d at 1060.*"

"In this case, the [] awardees will develop and test the devices proposed in their applications. *See, e.g.*, NSF Award No. 1444240 ("Annual and Final project reports, [], should document all efforts and outcomes, whether or not they are successful."). Government funding of research that will lead to the development and testing of an accused device supports a reasonable inference that the Government impliedly sanctioned infringing activity."

"The relevant [awards] are being used to develop: "a portable smartphone attachment that can be used to perform sophisticated field testing to detect viruses and bacteria," 2/12/16 Am. Compl. ¶78; "[a device] that derives biological signals from your smartphone's accelerometer ...[and] [t]his information is useful to base medical diagnoses in real-life conditions and to help track chronic health conditions and effects of therapeutic interventions," 2/12/16 Am. Compl. ¶80; "a cradle and app for the iPhone to make a handheld biosensor that uses the phone's own camera and processing power to detect any kind of biological molecules or cells," 2/12116 Am. Compl. ¶92; a handheld instrument to help contain the spread of Ebola, HIV, Tuberculosis, and Malaia, 2/12/16 Am. Compl. ¶102; "[a portable device for] real-time detection of explosives, toxicants, and radiation," 2/12/16 Am. Compl. ¶122; "highly sensitive rapid medical diagnostic tests," 2/12/16 Am. Compl. ¶126."

"Viewed in the light most favorable to Plaintiff, the February 12, 2016 Amended complaint alleges sufficient facts to raise a plausible right of relief under section 1498(a). See *Iqbal*, 556 U.S. at 677. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged."

"For the reasons discussed herein, the Government's June 24, 2016 Motion to Dismiss Certain Devices, pursuant to RCFC 12(b)(1) and 12(b)(6), is denied."

Since Judge Bruggink's Decision in *Golden v. Us* Case No. 13-307C; Nine Federal Judges Infer the United States Directly Infringed Golden's Patented Inventions Combinations

Judge	Case Number	Case Title	Court	Filed - Closed
Judge Bruggink	1:2013cv00307	Golden v. USA	U.S. Court of Federal Claims	05/01/2013 - ***11/10/2021***
Judge(s)	**Case Number**	**Case Title**	**Court**	**Filed - Closed**
Three Appellate Judges	2022cvpri01267	Golden v. Google LLC	U.S. Court Of Appeals, Federal Circuit	12/16/2021- ***09/08/2022***
One District Judge	3:2023cv00048	Golden v. Samsung Electronics America, Inc.	California Northern District Court	01/05/2023- ***06/08/2023***
Three Appellate Judges	2023cvpri02120	Golden v. Samsung Electronics America, Inc.	U.S. Court Of Appeals, Federal Circuit	07/07/2023- ***02/12/2024***
One District Judge	3:2022cv05246	Golden v. Google LLC	California Northern District Court	09/14/2022- ***04/03/2024***
One District Judge	3:2022cv05246	Golden v. Google LLC	California Northern District Court	09/14/2022- ***04/03/2024***

The doctrine of *Jes Judicata* [issue preclusion] prevents relitigating of factual issues already decided "if the identical issue was determined by a prior final judgment, and the party estopped had a fair opportunity and incentive to litigate the issue in a prior proceeding." *Portland Water Dist.*, 940 A.2d at 1100 (citation omitted). The question is, "how many more Judges' decisions does it take to know, the Government's "manufacture" of the product(s) asserted in this case, that senses for CBRNE, infringes Golden's patented inventions combinations?

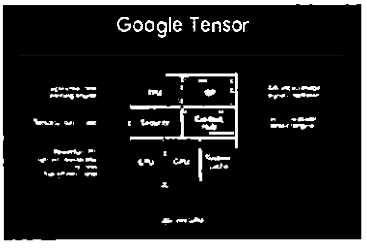
APPELLANT WILL ARGUE THE GOVERNMENT ADMITS ITS OWN LIABILITY

Golden owns the patent rights for a smartphone [communication device] that comprises a central processing unit; a central processing unit designed specifically for the smartphone. Golden has demonstrated throughout this case that the Google smartphone has to be "*modified*" with Golden's patented CPUs in order to function; meaning, in order to function as a communicating, monitoring, detecting, and controlling (CMDC) device [i.e., a smartphone].

Golden's patented CPUs, or Central Processing Units, are often referred to as the "brain" of the smartphone [Google smartphone]. They are responsible for executing instructions and performing calculations necessary for the functioning of the system. The CPU consists of various components, including the control unit, arithmetic logic unit (ALU), and cache memory.

Golden's patented CPUs operates a set of instructions stored in memory, commonly referred to as a program. The CPUs fetches these instructions, decodes them, performs the necessary operations, and stores the results back in memory.

The Google Tensor is a Google-designed system-on-chip (SoC/CPU) that first began in April 2016, after the introduction of the company's first Pixel smartphone. Begiuning in 2017, Google began to include custom-designed co-processors in its Pixel smartphones.

Google Tensor CPU	
	Google's alleged infringing smartphone device(s) must be *"modified"* by Google with the alleged infringing Google Tensor CPU; recognized as the *"brains"* of the alleged Google smartphone device(s); responsible for carrying out the operational and functional instructions of the Google smartphone device(s) in order to *"perform substantially the same function"*; in *"substantially the same way"*; to achieve *"substantially the same result"*; as Golden's patented CMDC device(s), that includes Golden's patented central processing units (CPUs).

Golden's patented CPUs primary role is to handle general-purpose tasks that require complex calculations and rapid decision-making. The CPUs execute instructions related to operating system operations, software applications, and managing various hardware components; tasks such as running programs, performing mathematical calculations, handling system requests, and managing memory allocation all fall under the responsibilities of the CPU(s).

Golden's patented CPUs are the central components that carries out the instructions necessary for the Google smartphones to function. Without Golden's patented CPUs [invented for smartphones] the Google smartphones, would not be able to execute tasks or process data.

DHS S&T "*Cell-All*"

Spearheaded by DHS S&T, *Cell-All* equips cell phones with a sensor capable of detecting deadly chemicals [CBRNE] … In 2007, S&T called upon the private sector to develop concepts of operations. To this end, teams from Qualcomm, NASA, Synkera, SeaCoast, and Rhevision Technology begin perfecting CBRNE sensing, data transfer, and wireless "***ubiquitous***" network connectivity. DHS S&T entered into cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, accelerated the commercialization of technology developed for government purposes.

In *Zoltek V*, the appellate court emphasized that§ 1498(a) is "its own independent cause of action" with three elements to trigger government liability: (1) the invention must be claimed in a patent; (2) it must be "used or manufactured by or for the United States," meaning each limitation of the claims must be present in the accused product or process; and (3) the "use or manufacture" of the patented invention must be done without license or lawful right—i.e., "use of an invention that, if done by a private party, would directly infringe the patent." 672 F.3d at 1321, 1323.

Judge Bruggink was fully aware that element (2) for triggering government liability could not be satisfied when the case is redirected to a dispute between private parties and the sensors and CPUs were not allowed because they were not *native* to the manufacture of Apple products.

Golden alleges the DHS continues to allow Qualcomm to appropriate and use; [and "collect a 5% running royalty on the price of each OEMs' smartphone sold" *FTC v. Qualcomm* Case 5:17-cv-00220-LHK Dkt. 1490 Filed 05/21/19], Golden's patented CMDC device, and CPU inventions without compensation. *See, James v. Campbell*, 104 U.S. 356, 357 (1882).

DoD DTRAATAK—CBRNE Plugin Sensors

The Android Team Awareness Kit (ATAK) is an Android smartphone geospatial infrastructure and military situation awareness app for Google, Samsung, LG, Qualcomm, etc. ATAK has a CBRNE plugin architecture which allows developers to add functionality.

The TAK has various mapping applications and end-user versions such as the iTAK that is built on Apple's iOS operating system; ATAK that is built on Google's android open-source operating system; and, WinTak that is built on Microsoft's operating system.

Also, the ATAK itself has various end-user versions: ATAK - Civilian (ATAK-CIV); ATAK - Government (ATAK-GOV); and, ATAK - Military (ATAK-MIL). See chart Below:

iTAK	ATAK				WinTAK	
Apple iPhone 12 Smartphone	Google Pixel 5 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Qualcomm Smartphone/ Snapdragon Insiders	Samsung Galaxy Book2 Pro 360 [PC or Tablet Mode]	HP ZBook Fury G8 Mobile PC Workstation
						

The DoD DTRA ATAK initiative combines Golden's patented CMDC device, CPU, and Multi-Sensor Detection device. The DoD DTRAATAK initiative also expands "***ubiquitous***" CBRNE sensing, with the use of consumer devices *i.e.*, laptops, PCs, tablets, and smartwatches, that are covered under Golden's patents, but were not asserted in the *Cell-All* initiative.

In *Zoltek V*, the appellate court emphasized that§ 1498(a) is "its own independent cause of action" with three elements to trigger government liability: (1) the invention must be claimed in a patent; (2) it must be "used or manufactured by or for the United States," meaning each

limitation of the claims must be present in the accused product or process; and (3) the "use or manufacture" of the patented invention must be done without license or lawful right—i.e., "use of an invention that, if done by a private party, would directly infringe the patent."

Judge Bruggink was fully aware that element (2) for triggering government liability could not be satisfied when the case is redirected to "issue preclusion" and the various iTAK, ATAK, and WinTAK apps that are built on the various Apple, Google, and Microsoft operating systems, cannot function without being integrated with Golden's patented central processing units (CPUs).

Golden alleges the DoD DTRA continues to appropriate and use Golden's patented inventions combinations of a CMDC device, CPU, and Detection device, without compensation. *See, e.g., James v. Campbell*, 104 U.S. 356,357 (1882).

DoD "JPEO-CBRND"

Draper Laboratory has been awarded a $26 million (all options) contract by the U.S. Department of Defense (DOD) to further expand the capabilities of its unmanned autonomous systems (UAS) software to perform CBRN reconnaissance missions.

Draper Laboratory ("Draper") will integrate flight software and sensor-driven algorithms that enable teams of unmanned systems to autonomously conduct CBRN missions.

The autonomous software on the aerial unmanned platform will be designed to operate with the command-and-control user interface for the U.S. Army's Nuclear, Biological and Chemical Reconnaissance Vehicle (NBCRV) Stryker platform currently being developed by Teledyne FLIR.

Under a $26 million contract with JPEO-CBRND, Draper will advance the development of its unmanned autonomous system so that it can operate in team formations and degraded operating environments. Pictured is Draper's UAS on a CBRN reconnaissance mission as viewed on a TAK-enabled device. Credit: Draper. The TAK-enable devices include smartphones, laptops, PCs, smartwatches, etc.

Draper's UAS on a CBRN reconnaissance mission includes a TAK-enabled consumer [cell phone, smartphone, laptop, PC, tablet or smartwatch] device wireless "***ubiquitous***" network connectivity. Draper will advance its system under an effort at JPEO-CBRND called CSIRP,

which stands for CBRN Sensor Integration on Robotic Platforms. Additional enhancements to the system will include advances in CBRN sensors.

In *Zoltek V,* the appellate court emphasized that§ 1498(a) is "its own independent cause of action" with three elements to trigger government liability: (1) the invention must be claimed in a patent; (2) it must be "used or manufactured by or for the United States," meaning each limitation of the claims must be present in the accused product or process; and (3) the "use or manufacture" of the patented invention must be done without license or lawful right—i.e., "use of an invention that, if done by a private party, would directly infringe the patent." 672 F.3d at 1321, 1323.

Judge Bruggink was fully aware that element (2) for triggering government liability could not be satisfied when the case is redirected to "issue preclusion" and the unmanned autonomous systems (UAS) software to perform CBRN reconnaissance missions that are built on the various Apple, Google, and Microsoft operating systems, cannot function without being integrated with Golden's patented central processing units (CPUs).

Golden alleges the DoD DTRA continues to appropriate and use Golden's patented inventions combinations of a CMDC device, CPU, Detection device, and Pre-programed Stop, Stall, Vehicle Slow-down system, without compensation. *See, e.g., James v. Campbell,* 104 U.S. 356, 357 (1882).

The Fifth Amendment of the United States Constitution

"No person shall be [] deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.": The Fifth Amendment provides that no person shall be deprived of life, liberty, or property, without due process of law. *U.S. Const. amend. V.*

U.S. Supreme Court

In *James v. Campbell,* 104 U.S. 357 (1881), this Court said: "That the Gov't of the United States, when it grants letters patent for a new invention or discovery in the arts, confers upon the patentee an exclusive property in the patented invention which cannot be appropriated or used by the government itself without just compensation, any more than it can appropriate or use without compensation land which has been patented to a private purchaser we have no doubt."

APPELLANTWILLARGUE THE GOVERNMENT'S WORSENING OF EARLIER CONDITIONS

The United States Court of Federal Claims ["the Government's Court] Judge, was "*precluded*" under 28 U.S. Code § 144 - Bias or prejudice of judge, from adjudicating the current case and entering a final decision. Golden filed a timely motion for disqualification under 28 U.S. Code§ 144 for racial bias and bias in favor of the Government that the Judge ignored and allowed to set on the docket for seven months.

The Government is "*precluded*" by the United States Supreme Court from appropriating or using Golden's patented invention(s) without just compensation: "In *James v. Campbell*, 104 U.S. 356, 357-58 (1882), the Supreme Court explained that when the government grants a patent, it "confers upon the patentee an exclusive property in the patented invention which cannot be appropriated or used by the government itself, without just compensation."

The Government is "*precluded*" by the Fifth Amendment Clause of the United States Constitution from depriving Golden of his property without paying just compensation: "No person shall ... be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." [U.S. Cons't. amend. V]

The United States Court of Federal Claims ["the Government's Court] is "*precluded*" by the Tucker Act (March 3, 1887, ch. 359, 24 Stat. 505, 28 U.S.C. § 1491) from adjudicating outside the Court's jurisdiction, Golden's money-mandating claims against the Government: "While the Tucker Act confers jurisdiction on the Court of Federal Claims and ... authorizes money claims against the government "founded either upon the Constitution, or any Act of Congress, or any regulation of an executive department, or upon any express or implied contract with the United States . . . The statute provides the right to file a lawsuit to obtain a monetary remedy, while leaving the content of the legal claim to the Constitution..."

The Government is "*precluded*" by Title 28 of the United States Code; Section 1498 from using or manufacturing Golden's inventions without license; the lawful right; or reasonable and entire compensation: "Whenever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture... the use or manufacture of an invention

described in and covered by a patent of the United States by a contractor, a subcontractor, or any person, firm, or corporation for the Government and with the authorization or consent, shall be construed as use or manufacture for the United States." [28 U.S. C § 1498(a)]

The Government is "*precluded*" by the Federal Circuit in *Zoltek V* from requiring Golden to prove direct infringement of Apple and Google products under 35 U.S.C. § 271(a) as a necessary predicate to proving direct infringement by or for the Government under 28 U.S.C. § 1498(a): "[I]n the 2012 *en banc* decision *Zoltek V,* the Federal Circuit abrogated *Zoltek III,* holding that establishing conduct falling within the definition of direct infringement codified in 35 U.S.C. § 271(a) is not a predicate to finding infringement under§ 1498(a)... In *Zoltck V,* the appellate court emphasized that§ 1498(a) is "its own independent cause of action" with three elements to trigger government liability: (1) the invention must be claimed in a patent; (2) it must be "used or manufactured by or for the United States," []; and (3) the "use or manufacture" of the patented invention must be done without license or lawful right—i.e., "use of an invention that, if done by a private party, would directly infringe the patent."

The Government is "*precluded*" by the Bayh-Dole Act, from extending its license to practice Golden's inventions for commercial use by third-parties to compete with Golden on the open market: "While the Government retains a royalty-free license under the Bayh–Dole to practice the invention under the Bayh–Dole Act, the right is limited to practice "for or on behalf of the United States." Therefore, the license does not extend to commercial use by third parties. For example, the government's license could not be used to allow a third party to practice the inventing party's invention and thereby compete with the inventing party on the open market."

The Government is "*precluded*" by the US Court of Appeals for the Federal Circuit from limiting or restricting the components [elements] of the alleged infringing products to those "*native*" to the manufacture of the Apple and/or Google products: "In *FastShip, LLC v. United States,* the US Court of Appeals for the Federal Circuit held that to be manufactured under 28 U.S.C. Section 1498, an accused product must include each claim limitation so it is "suitable for use" ... [T]he Federal Circuit interpreted the term "manufactured" in Section 1498:

- According to its ordinary, contemporary, common meaning, ruling that the plain meaning of "manufactured" encompasses products made or worked into a form that is suitable for use.
- In the context of the overall statutory scheme, concluding that interpreting "manufactured" so the product must be suitable for use aligns with the Federal Circuit's

prior interpretation of "use" in Section 1498 requiring each claim limitation to be present in the thing invented.

The Government is "*precluded*" by the United States Supreme Court from extending the preclusion doctrines to include a new freestanding preclusion doctrine—the *Kessler* Doctrine: "In May 2020, the Supreme Court decided the case of *Lucky Brand Dungarees, Inc. v. Marcel Fashions Grp., Inc.*, 140 S. Ct. 1589 (2020) and expressly refused to extend preclusion doctrines beyond their traditional bounds set by the doctrines of issue and claim preclusion. The Supreme Court has repeatedly held that, absent guidance from Congress, courts should not create special procedural rules for patent cases or devise novel preclusion doctrines that stray beyond the traditional bounds of claim and issue preclusion. Nonetheless, over the past several years, the Federal Circuit has created and then repeatedly expanded a special, patent-specific preclusion doctrine that it attributes to the Supreme Court's 114-year-old decision in *Kessler v. Eldred*, 206 U.S. 285 (1907)—a case the Court has not cited for almost 70 years.

Absent guidance from Congress, the Government in this case has devised a way to stray beyond the traditional bounds of claim and issue preclusion, to create a new freestanding preclusion doctrine [*Kessler*] that may apply even when claim and issue preclusion do not. The freestanding *Kessler* doctrine does not supersede the Constitutional provisions of the Fifth Amendment "No person shall... be deprived of life, liberty, or property, without due process of law;" and the freestanding doctrine do not supersede Congress intent in creating the statute for patent infringement under 28 U.S.C. § 1498(a).

The United States Court of Federal Claims ["the Government's Court] is "*precluded*" by the doctrine of *vertical stare decisis* from dishonoring the precedence set by the higher United States Court of Appeals for the Federal Circuit in two separate cases within the Federal Circuit's jurisdiction: "Vertical stare decisis is the rule binding a lower court to adhere to the decisions of higher courts in its jurisdiction. Under the doctrine vertical stare decisis it is a court's obligation to follow the precedence of a superior court; and, under the doctrine horizontal stare decisis, a court's obligation to follow its own precedence. Vertical stare decisis is an inflexible rule that admits of no exception. *See Rodriguez de Quijas v. Shearson/Am. Express, Inc.*, 490 U.S. 477, 484 (1989). See chart below:

- The United States Court of Appeals for the Federal Circuit Judges in *Golden v. Google, LLC*, Case No. 22-1267; determined Direct Infringement by or for the Government, arises when there's a combined ATAK Software; CBRN Plugins; CPU; and Smartphone

- The United States Court of Appeals for the Federal Circuit Judges in *Golden v. Samsung* Case No. 23-2120; agreed with the Northern District of California Court Judge in *Golden v. Samsung* that Direct Infringement by or for the Government arises when there's a combined ATAK Software; CBRN Plugins; CPU; and Smartphone

In *Golden v. Samsung Electronics America, Inc.* Case No. 23-0048; and in *Golden v. Google LLC* Case No. 22-5246 the Courts determined, "direct infringement by or for the Government arises when there's the combinedATAK Software; CBRN Plugins; CPU; and Smartphone.

This determination was made after the decision in the lead case *Golden v. USA* no. 13-307C on 11/10/2021. Therefore, dismissing for issue preclusion is perceived as moot. The dismissal of this current case *Golden v. Google* No. 23-811C on appeal is not "on the merits" if the dismissal is for issue preclusion of a case perceived as *moot*, and higher Courts decided in the opposite.

Also, the decisions of the higher United States Court of Appeals for the Federal Circuit made in *Golden v. Google LLC* Case No. 22-1267 and in *Golden v. Samsung Electronics America, Inc.* Case No. 23-2120 that was decided, "direct infringement by or for the Government arises when there's the combinedATAK Software; CBRN Plugins; CPU; and Smartphone", is binding precedence under the doctrine of *vertical stare decisis*. The United States Court of Federal Claims is duty bound to attempt faithfully to apply the precedents of the Federal Circuit.

Judge(s)	**Case Number**	**Case Title**	**Court**	**Filed-Closed**
Judge Bruggink	1:2013cv00307	Golden v. USA	U.S. Court of Federal Claims	05/01/2013-***11/10/2021***
Judge(s)	**Case Number**	**Case Title**	**Court**	**Filed - Closed**
Three Appellate Judges	2022cvpri01267	Golden v. Google LLC	U.S. Court of Appeals, Fed. Cir.	12/16/2021-***09/08/2022***
One District Judge	3:2023cv00048	Golden v. Samsung, Inc.	California Northern District Court	01/05/2023-***06/08/2023***
Three Appellate Judges	2023cvpri02120	Golden v. Samsung Inc.	U.S. Court of Appeals, Fed. Cir.	07/07/2023-***02/12/2024***
One District Judge	3:2022cv05246	Golden v. Google LLC	California Northern District Court	09/14/2022-***04/03/2024***
One District Judge	3:2022cv05246	Golden v. Google LLC	California Northern District Court	09/14/2022-***04/03/2024***

CONCLUSION

I understand that as a *ProSe* Black and/or African American trying to find equal justice in a judicial system of systemic and structural racism, I have a lot working against me when the system is bias in favor of large corporations, and bias against inventors who looks like me.

Robert Kearns, representing himself [*ProSe*], devoted thirty years defending himself against large corporations for his intermittent windshield wiper invention. He finally won his case but it was twelve (12) years before the case made it to trial.

Dred Scott was an enslaved African American man who, along with his wife, Harriet, unsuccessfully sued for the freedom of themselves and their two daughters. In a landmark case, the United States Supreme Court decided 7–2 against Scott, finding that neither he nor any other person of African ancestry could claim citizenship in the United States, and therefore Scott could not bring suit in federal court under diversity of citizenship rules. It took President Abraham Lincoln's Emancipation Proclamation in 1863 and the post-Civil War Reconstruction Amendments—the Thirteenth, Fourteenth and Fifteenth amendments—to nullify the decision.

This is the fourth time Judge Bruggink has deprived me of my property without due process of law and just compensation. The Supreme Court ruled in *James v. Campbell*, 104 U.S. 356, 358 (1882) that "the Government cannot appropriate or use a patented invention(s) without just compensation'. In my case the Government has done just that for almost twenty (20) years. I just simply want to Panel to look me in the face and tell me the law does not apply to someone who looks like me, and that they are complicit with the rulings of a racist Judge Bruggink. The Government continue the use my patented inventions without compensation. [***Exhibits A, B, C***]

28 U.S.C. § 1498(a) is "its own independent cause of action"

In *Zoltek III,* the Federal Circuit further narrowed§ 1498 by holding that direct infringement under§ 1498(a) with respect to the United States' use or manufacture of a patented invention was predicated on § 271(a) of the Patent Act. See *Zoltek Corp. v. United States* (*Zoltek II*), 442 F.3d 1345, 1350 (Fed. Cir. 2006), abrogated by *Zoltek V*, 672 F.3d 1309, 1322–23 (Fed. Cir. 2012) (en bane); *see* also *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1316 (Fed. Cir. 2005) ("[D]irect infringement under section 271(a) is a necessary predicate for government liability under section 1498."); *Motorola, Inc. v. United States*, 729 F.2d 765, 768 n.3 (Fed. Cir. 1984).

However, in the 2012 *en banc* decision *Zoltek V*, the Federal Circuit abrogated *Zoltek III*, holding that establishing conduct falling within the definition of direct infringement codified in 35 U.S.C. § 271(a) is not a predicate to finding infringement under§ 1498(a). Instead, the court concluded that the scope of § 1498(a) is "linked to the scope of the patent holder's rights as granted by the patent grant in title 35 U.S.C. section 154(a)(1)." *Zoltek V*, 672 F.3d at 1323. In contrast to the statutory definitions of infringement in § 271, § 154(a)(1):

> . . . the right to exclude others from using, offering for sale or selling throughout the United States, products made by that process, referring to the specification for the particulars thereof. 35 U.S.C. § 154(a)(1)."

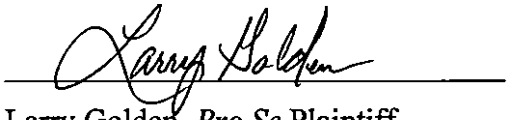
The Fifth Amendment of the United States Constitution

"No person shall be [] deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.": The Fifth Amendment provides that no person shall be deprived of life, liberty, or property, without due process of law. *U.S. Const. amend. V.*

U.S. Supreme Court

In *James v. Campbell*, 104 U.S. 357 (1881), this Court said: "That the Gov't of the United States, when it grants letters patent for a new invention or discovery in the arts, confers upon the patentee an exclusive property in the patented invention which cannot be appropriated or used by the government itself without just compensation, any more than it can appropriate or use without compensation land which has been patented to a private purchaser we have no doubt."

Sincerely,

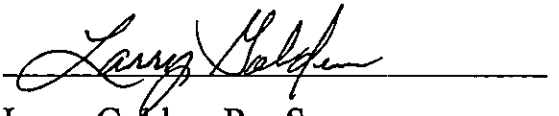


Larry Golden, *Pro Se* Plaintiff
740 Woodruff Rd., #1102
Greenville, SC 29607
(B) 8649927104
Email: atpg-tech@charter.net

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 18th day of January, 2025, a true and correct copy of the foregoing "Plaintiff-Appellant's Motion for Oral Argument", was served upon the following Defendant by priority "express" mail:

GrantD. Johnson
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
Grant.D.Johnson@usdoj.gov
(202) 305-2513



Larry Golden, Pro Se
740 Woodruff Rd., #1102
Greenville, SC 29607
(M) 8649927104
Email: atpg-tech@charter.net

Exhibit A

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR DETECTION AND HOMELAND SECURITY

Dr. Eric C. Haseltine, Subcommittee Chair; Dr. James Decker, Dr. Marian Greenspan, Mr. Philip Coyle, Dr. Michael Goldblatt, Dr. Kathie Olsen, Dr. Gerald Parker White Paper for HSSTAC Quadrennial Homeland Security Review (QHSR) Subcommittee in support of the 2018 QHSR

The opportunity

Digital devices connected to the global network are rapidly finding their way into almost every facet of life. In addition to computers, smart phones, tablets, game consoles, new categories of connected devices such as fitness wearables, digital fashion accessories, Internet of Things (IOT) appliances, security systems, self-driving cars, robotics, smart toys, industrial control and home automation systems are coming on the market at an accelerating pace. Over the next decade, these connected devices and others, such as Augmented Reality systems and telemedicine sensors will continue to penetrate new niches. All of these connected devices have sensors of one kind or another (e.g. accelerometers, GPS, RF sensors, cameras & microphones) so that it will be theoretically possible to "instrument" virtually the entire population of the U.S. in one form or another, and to use this synoptic instrumentation to swiftly detect and respond to CBRN events.

The Priorities

- Mobile apps can combine sensor feeds from many handsets to create vast "synthetic apertures" to detect earthquakes (from accelerometer data), explosions (from microphones) and even gamma radiation (from activation of cell cameras).
- Sensor activity from cameras, microphones, accelerometers in mobile devices, laptops, computers and IOT devices (home security/automation, municipal, industrial) can detect, localize and sometimes identify CBRN events, including those producing ionizing radiation.
- Mobile GPS data (and cell/sector handshaking data) can identify handsets that were exposed to pathogens, toxins and radioactive material so that (with suitable civil liberties protections) affected individuals (and people the individuals later meet) can be found and treated.
- Personalized, localized text messaging to mobile devices can instruct affected individuals (detected as just described) to seek help, avoid spreading toxins or disease or where to seek shelter or protection from a recent or imminent event in specific locations.
- Mandates for mobile device emergency modes and applications (e.g. radiation detection, exploitation of other sensors from native Apps in all handsets).

Homeland Security
Science and Technology

Homeland Security Science and Technology Advisory Committee (HSSTAC): Quadrennial Homeland Security Review Subcommittee

Chemical, Biological, Radiological, and Nuclear Detection White Paper

March 10, 2017

Homeland Security
Science and Technology

This publication is presented on behalf of the Homeland Security Science and Technology Advisory Committee, Quadrennial Homeland Security Review Subcommittee, Chemical, Biological, Radiological, and Nuclear Detection, chaired by Eric Haseltine with contributions from Dr. Gerald Parker, Dr. Yacov Haimes, Mr. Daniel Dubno as part of recommendations to the Department of Homeland Security, Under Secretary for Science and Technology, Robert Griffin (*Acting*).

<Signature on File>

Eric Haseltine
President
Haseltine Partners, L.L.C.

HSSTAC Staff: Michel Kareis, HSSTAC Executive Director/DFO and Gretchen Cullenberg, QHSR Subcommittee support.

Homeland Security
Science and Technology

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR DETECTION AND HOMELAND SECURITY

Dr. Eric C. Haseltine, Subcommittee Chair; Dr. James Decker, Dr. Marian Greenspan, Mr. Philip Coyle, Dr. Michael Goldblatt, Dr. Kathie Olsen, Dr. Gerald Parker

White Paper for HSST.AC Quadrennial Homeland Security Review (QHSR) Subcommittee in support of the 2018 QHSR

Digital "ripples" from connected devices can help detect and manage CBRN events

Introduction

There is room for improvement in our ability to detect, locate and identify chemical, biological, radiological and nuclear defense (CBRN) events in the Homeland, and to differentiate such willful events from "natural" occurrences such as infectious disease outbreaks or hazardous materials (HAZMAT) releases. Further, to contain the damage from CBRN terrorism, it would be desirable to identify everyone that a CBRN event has affected, along with where those affected individuals subsequently go.

The opportunity

Digital devices connected to the global network are rapidly finding their way into almost every facet of life. In addition to computers, smart phones, tablets, game consoles, new categories of connected devices such as fitness wearables, digital fashion accessories, Internet of Things (IOT) appliances, security systems, self-driving cars, robotics, smart toys, industrial control and home automation systems are coming on the market at an accelerating pace. Over the next decade, these connected devices and others, such as Augmented Reality systems and telemedicine sensors will continue to penetrate new niches. All of these connected devices have sensors of one kind or another (e.g. accelerometers, GPS, RF sensors, cameras & microphones) so that it will be theoretically possible to "instrument" virtually the entire population of the U.S. in one form or another, and to use this synoptic instrumentation to swiftly detect and respond to CBRN events.

One way to think about this opportunity is to view the data flows created by interconnected devices as rivers of bits that feed an immense ocean of bits containing vast, up-to-the-moment information about the human condition. Events that cause social disruption leave ripples and wakes in this digital ocean. And, just, as different kinds of vessels produce different kinds of wakes, different kinds of social disruptions produce unique digital signatures that can help identify the nature of the disruption, along with its time and place. In some cases, sophisticated analysis can also pinpoint who *caused* the disruption. Finally, most promising of all are

opportunities to detect "bow waves" of disruption that *precede* a CBRN event, so that the event might be prevented from occurring in the first place.

Maintaining both the appearance and fact of privacy while collecting and acting on streaming data from billions of connected sensors in our population, will be essential to realizing this vision. Fortunately, innovative approaches to preserving privacy—such as machine learning applied to pooled, anonymized data, are fast emerging to address this challenge.

Accordingly, all the proposed approaches that follow assume that privacy must be protected, and *will* be protected using these emerging techniques.

Candidate approaches

A multi-billion-dollar industry has already emerged to detect and act upon digital "wakes" and "bow waves." For example:

- A contractor to the NFL has analyzed localized Twitter feeds to detect fights in stadiums during games *before* stadium operators themselves knew of the fights.
- A financial technology (Fintech) company has analyzed pooled, anonymized data from cell operators (including GPS and other location data) to predict moves in equities and commodities markets based on changes in the movements and pattern of life of workers in financial districts.
- Health officials in Africa have used similar data to identify sources and vectors for spread of Dengue fever and Ebola.
- Georgetown University has detected flu outbreaks in Asia weeks ahead of the World Health Organization by scraping and analyzing digital and social media.
- Foreign Policy analysts can sometimes predict and localize political demonstrations from the volume and location of mobile text and social media posts (purchased in anonymized form).
- Mobile apps can combine sensor feeds from many handsets to create vast "synthetic apertures" to detect earthquakes (from accelerometer data), explosions (from microphones) and even gamma radiation (from activation of cell cameras).

Detecting CBRN events

These kinds of techniques can be adapted to detecting CBRN events as follows:

- Changes in pattern of life manifested in GPS movement and accelerometer movement in mobile and wearable devices
    - Rapid movement away from (or towards) a location.
    - Sudden loss of connectivity to multiple mobile devices in a location.
    - Changes, over time, of accelerometer data indicating reduced physical activity or slowed physical activity due to illness or impairment. Changes in data from fitness wearables measuring heart rate, number of steps and other physiological signals.

- Analysis of content of social media posts, and traffic analysis of anonymized, but localized messaging to identify location and nature of CBRN event.
- Sensor activity from cameras, microphones, accelerometers in mobile devices, laptops, computers and IOT devices (home security/automation, municipal, industrial) can detect, localize and sometimes identify CBRN events, including those producing ionizing radiation.
- Techniques for analyzing such data (that are beyond the scope of this document) can sometimes identify who had prior knowledge of a CBRN event and even predict an event before it occurs.
- Machine learning technology can sometimes, based on analysis of historical events, differentiate between natural (e.g. disease/HAZMAT) and intentional acts.
- Spikes in internet search volume for keywords describing an event (such as explosion) can be detected minutes after the event.
- IOT smoke detectors can be easily modified to detect localized increases in ionizing radiation (detecting radiological events and possibly the presence of fissionable material *before* the material detonates).

Managing CBRN events

- Mobile GPS data (and cell/sector handshaking data) can identify handsets that were exposed to pathogens, toxins and radioactive material so that (with suitable civil liberties protections) affected individuals (and people the individuals later meet) can be found and treated.
- Personalized, localized text messaging to mobile devices can instruct affected individuals (detected as just described) to seek help, avoid spreading toxins or disease or where to seek shelter or protection from a recent or imminent event in specific locations.
- Connected sensors can localize events so that first responders know where to go.
- Emotional sentiment analysis, examining content of electronic messages and posts, can indicate level of panic and effectiveness of government emergency messaging.
- Digital "bow waves" and "wakes" can sometimes pinpoint who caused a CBRN event so that law enforcement and security officials can "find, fix and finish" the perpetrators.

Recommended next steps for DHS

There are many technical challenges to collecting, analyzing and acting upon digital "bow waves" and "wakes." But early work in commercial sector suggests that these challenges can and will be surmounted, and that DHS can take advantage of these rapid advances through a multi-step process as follows:

Engage data scientists in DHS S&T and other stakeholders at DHS to:

- Prioritize gaps in detection, identification, localization and attribution of CBRN events.
- Survey leading ongoing efforts and players in the private sector that can bridge these gaps.
- Identify the most promising near-term applications.

- Begin pilot programs.
- Look for ways to exploit these new technologies for other pressing DHS needs such as border protection, counter-terrorism and natural disaster management.
- Look for ways to integrate "digital ocean" sensing and analytics with existing DHS sensors and analytics.

As important as these S&T efforts will be, they pale in importance to the daunting policy challenges associated with collecting, analyzing and acting upon disturbances in the digital "ocean."

Accordingly, in parallel with the S&T initiatives, DHS should Identify & develop approaches for sensitive policy issues, including:

- Privacy.
- Meta-data standards for "connecting dots" among diverse digital devices data streams and cloud storage sources.
- Access to private data (e.g. cell carriers, ISPs).
- Mandates for mobile device emergency modes and applications (e.g. radiation detection, exploitation of other sensors from native Apps in all handsets).
- Mandates for new features in networked IOT devices (e.g. detecting and reporting increases in ionizing radiation in smoke detectors).
- Public messaging and education to convince the population both of the need for such measures and that privacy can and will be protected.
- How to take advantage of classified data and techniques to augment unclassified initiatives, without compromising national security.

Exhibit B

APPELLANT WILL ARGUE THE SPECIFICATIONS OF THE THREE INITIATIVES: THE DHS S&T *CELL-ALL* INITIATIVE; THE DOD DTRA iTAK, ATAK & WinTAK CBRNE INITIATIVES; and, THE DOD JPEO-CBRND INITIATIVE, ARGUED IN THIS CASE WAS FIRST REQUESTED IN THE DHS SBInet INITIATIVE

The fate of SBInet had been in question since DHS Secretary Janet Napolitano ordered an assessment of the project in January 2010 and in March 2010 froze additional funding for anything beyond already begun initial deployments. On Jan. 14, 2011, DHS said it would redirect funding originally intended for SBInet—including fiscal 2011 SBInet funds—to the new border security technology effort.

Israeli defense firm wins $145 million contract from US Department of Homeland Security.

By YAAKOV LAPPIN MARCH 2, 2014 15:55

Israeli defense firm Elbit has been awarded a $145 million contract by the US Department of Homeland Security to construct a series of surveillance towers on Arizona's border with Mexico, the company announced on Sunday. The project, called Integrated Fixed Tower Project (IFT), plans to see security posts equipped with radars and cameras that can detect human movement spring up along the American state's southern frontier. The work is to be carried out by Elbit's US subsidiary, Elbit Systems of America, which is based at Fort Worth, Texas. Construction of the towers will take around a year, the company said. It declined to provide further details.

Last week, Republican Senator John McCain of Arizona, released a statement welcoming the contract. "Arizonans have been waiting more than a decade for the Department of Homeland Security (DHS) to place the needed technology along our border to support the Border Patrol and fully secure our southern border," he said. "After many months of delay, the awarding of this contract to Elbit Systems of America is an important development toward fully securing the border in Arizona. If this technology is developed, integrated and fielded correctly, these Integrated Fixed Towers in southern Arizona, coupled with the tremendous work of the Border Patrol, will give our agents the ability to detect, evaluate and respond to all illegal entries crossing our border," McCain stated. "The American people have long expected us to secure our borders. The awarding of this contract is a step in the right direction."

In May, the US-based Defense News website reported that "the IFT program is an ambitious attempt to install a series of surveillance towers along the US/Mexico border. The idea is to deploy a series of networked, integrated fixed towers equipped with radar and cameras that will 'be able to detect a single, walking, average- sized adult' at a range of 5 miles [8 km.] to 7.5 miles [12 km.] during day or night, while sending close to real-time video footage back to agents manning a command post." Defense News added that the IFT program comes after a previous border security program, called the Secure Border initiative (SBI), was canceled in 2011 despite the government spending $1 billion over the course of six years. That effort that saw just 85 km. of the 626-km. border covered by the program, the report said.

Elbit America Providing CBP with New Relocatable Surveillance Towers; Introduces Autonomous Tower System

*This article originally appeared in **Defense Daily** on Sept. 1, 2020. Reprinted here with permission.*

Elbit Systems of America is providing Customs and Border Protection (CBP) with new trailer-mounted intelligent surveillance towers that will fill in gaps for long-range surveillance on the southern border.

The 80-feet tall Intelligent Relocatable Long-Range Surveillance Tower is similar to the Integrated Fixed Tower (IFT) systems the company has provided CBP to enhance situational awareness along certain stretches of the U.S. southwest border, but the new system can be set up within a day for operations and then moved in response to the changing threat patterns, Joel Friederich, Vice President of C4I and Homeland Security Solutions at Elbit Systems of America, told HSR sister publication Defense Daily during a recent telephone interview.

More than 50 IFT systems have been deployed, Elbit said. Elbit Systems of America is the U.S. subsidiary of Israel's Elbit Systems [ESLT].

Like the IFT systems, the new Intelligent Relocatable Towers include electro-optic and infrared cameras for day and nighttime imaging, ground surveillance radar, and related communications. The systems feature limited artificial intelligence capabilities so that the sensors can detect and track a potential item of interest and then alert a Border Patrol agent.

The Border Patrol, an arm of CBP, uses Elbit's TORCH command and control platform to integrate IFT, the Intelligent Relocatable system and other border security sensor systems and technologies to create a common operating picture at the station level and for agents in the field.

Elbit said its new Autonomous Relocatable Surveillance Tower (ARST) system, which features more robust AI and machine learning capabilities than found in the Intelligent Relocatable Tower and IFT systems, was selected in April by the Defense Department's Combatting Terrorism Technical Support Office (CTTSO) for evaluations for DoD and CBP.

The ARST systems stand taller than the Intelligent Relocatable Towers, 110-feet, offering longer sensor ranges and a broader field of view, Friederich said. The higher-end AI capabilities on the ARST mean the systems can detect, track and identify an item of interest, taking the human out of the loop until necessary, he said.

So, if the ARST system sees something not of interest to CBP, it won't bother alerting an operator, Friederich said.

The AI enhancements allow the system to watch over more of the border with fewer agents, which means some agents can return to the field, Elbit said.

The CTTSO will begin evaluating the ARST in the first quarter of 2021 and the contract allows for the agency to procure additional systems if needed for more evaluation, he said.

The Intelligent Relocatable Towers will provide a bridge to the ARST systems, Friederich said. The technology behind the ARST systems could be swapped out for the control logic on an IFT system so the physical appearance of the surveillance system may look the same but the capabilities would be improved, he said.

The ARST can be deployed in less than two hours. The long-range payload includes ground surveillance radar, a high- resolution day camera, and thermal camera. The trailer provides electronic enclosures, security features and a power generator.

Friederich also said both the ARST and Intelligent Relocatable systems are modular and can be adapted to customer needs. Both systems also integrate into the company's TORCH system.

CBP currently purchases another AI-enabled surveillance tower system, the Autonomous Surveillance Tower (AST) system provided by Anduril Industries. The ASTs are also relocatable but are a shorter-range system, out to about a mile versus greater than seven miles for the ARST.

In a statement provided to HSR, CBP said "The Intelligent Relocatable Long-Range Surveillance Tower (IRLRST) is an Integrated Fixed Tower system mounted on an 80-foot relocatable tower. Elbit Systems developed this Trailer Mounted Surveillance System under the IFT program for potential use where fixed towers cannot be used due to environmental, real estate or other reasons. The Autonomous Relocatable Surveillance Tower (ARST) will utilize a sensor system similar to the IFT sensor system mounted on a 100-foot relocatable tower. Elbit Systems is developing the ARST for the Combating Terrorism Technical Support Office. The potential exists to use IRLRSTs and/or ARSTs on future CBP tower programs where long range, non-permanent deployment is desired. Conversely, 200 Autonomous Surveillance Towers (AST) will be deployed in areas where less range is required, there is no power or communications infrastructure, non-permanent deployment is desired, and manpower to operate surveillance systems is limited. The systems are complementary and will be utilized as the operational and environmental conditions dictate."

Fiber Optic Sensor Integrated into TORCH

Elbit Systems of America also said it has integrated a fiber optic-based system used for ground and underground surveillance along portions of the southern border into the TORCH command and control platform used by the Border Patrol.

The integration of Sintela's Linear Ground Detection Systems (LGDS) is another example of the flexibility of the company's TORCH system.

"Aided by the TORCH System's autonomy and artificial intelligence (AI), Border Patrol agents will be able to more safely and efficiently perform their national security duties," Friederich said in a statement. "We are pleased to partner with Sintela, making Elbit Systems of America now the exclusive U.S. distributor of their market leading and fully compliant LGDS system."

Elbit Systems of America has also integrated cameras, gimbals, laser range finders, laser pointers, radars, unattended ground sensors, and intelligent lighting for the border wall on the southern border into TORCH.

Friederich previously said Elbit's AI capabilities make it easy on users of TORCH by automatically identifying items of interest through sensors, linking different sensors together to track an event, and then automatically alerting agents if necessary.

Earlier this year, Customs and Border Protection, the parent agency for the Border Patrol, awarded Sintela a potential $6.4 million contract to maintain the LGDS, which is being used to enhance situational awareness for cross-border intrusions in support of the border wall system along certain parts of the southern border. Sintela is based in the United Kingdom and has an office in Houston.

"We feel strongly that the border surveillance technologies we've developed, especially their AI, autonomy and machine learning characteristics, could greatly benefit the DoD as they consider how to improve their force protection and base security capabilities," he said.

https://www.elbitamerica.com/news/elbit-america-providing-cbp-with-new-relocatable-surveillance-towers-introduces-autonomous-tower-system

Integrated Fixed Towers system will expand its deployment across the U.S. southern border

PR Newswire

FORT WORTH, Texas, June 26, 2019

FORT WORTH, Texas, June 26, 2019 /PRNewswire/ —Elbit Systems of America was awarded an approximately $26 million contract from the United States Customs and Border Protection (CBP) to install an Integrated Fixed Towers (IFT) system in the U.S. Border Patrol Casa Grande Area of Responsibility (AoR) in Arizona. The project will be performed over a one-year period. To date, Elbit Systems of America has been awarded a number of contracts from CBP to install IFT systems in numerous AoR's covering a total of approximately 200 miles of the Arizona-Mexico border.

The IFT system comprises a command-and-control center and a networked multi-tower, multi-sensor system that continuously monitors portions of the U.S. southern border. Information from the towers is sent to the command-and-control center and a Border Patrol Station providing agents with long-range, persistent surveillance and situational awareness that allows them to dispatch an appropriate response. This capability provides greater safety for the agents patrolling the border in the Casa Grande AoR.

President and Chief Executive Officer Ranaan Horowitz said, "Elbit Systems of America is honored to have been selected by the U.S. Customs and Border Protection and the Tohono O'odham Nation to provide a solution to suit the needs of those living and working along the border in the Casa Grande Area of Responsibility. This project clearly demonstrates our company's mission to provide innovative solutions that protect and save lives."

In addition to the company's Integrated Fixed Towers, Elbit Systems of America has developed a number of other border security measures and technology. More on these solutions is available at www.nextgenborder.com.

About Elbit Systems of America, LLC

Elbit Systems of America is a leading provider of high-performance products, system solutions, and support services focusing on the defense, homeland security, commercial aviation, and medical instrumentation markets. With facilities throughout the United States, Elbit Systems of America is dedicated to supporting those who contribute daily to the safety and security of the United States. Elbit Systems of America, LLC is wholly owned by Elbit Systems Ltd. (NASDAQ: ESLT and TASE: ESLT), a global high technology company engaged in a wide range of programs for innovative defense and commercial applications. For additional information, visit: www.ElbitAmerica.com or follow us on Twitter.

https://www.defensedaily.com/cbp-awards-new-surveillance-tower-contracts-to-atsc-gd-elbit/homeland-security/

CBP Awards New Surveillance Tower Contracts To ATSC, GD, Elbit

Customs and Border Protection has awarded contracts to three companies to provide new and upgraded surveillance towers to enhance border security, selecting **Advanced Technology Systems Company** (ATSC), **General Dynamics** [GD], and Elbit America for the work.

CBP announced the awards on Wednesday on the government business opportunities website *Sam.gov*, saying that Elbit's award is for $23.9 million, ATSC $23.4 million, and GD One Source, LLC, for $20.5 million.

The Integrated Surveillance Towers (IST) Consolidated Tower & Surveillance Equipment (CTSE) awards are for medium- and long-range surveillance towers and include various subsystems and sensors for U.S. Border Patrol agents to continuously detect, identify, classify, and track items of interest within each tower systems' coverage area along the southern and northern borders of the U.S.

CBP said it plans to acquire about 277 new IST towers in 53 separate Border Patrol areas of operation (AoRs) and upgrade about 191 legacy surveillance towers in 31 separate AoRs. Last December, CBP issued the solicitation for the IST CTSE program, saying the required surveillance capabilities include fixed and relocatable systems for short-, medium-, and long-range operations along the northern and southern borders and for maritime awareness.

Elbit America, part of Israel's **Elbit Systems** [ESLT], previously provided the long-range Integrated Fixed Towers (IFTs) to the Border Patrol and GD the medium- and short-range Remote Video Surveillance System (RVSS). The IFTs include cameras for day and night sensing, radar, and related communications. The RVSS systems include day and night cameras that Border Patrol agents control remotely.

ATSC, which is based in Northern Virginia, has provided security surveillance systems to the U.S. Army.

CBP also procures short-range border security surveillance towers from Anduril Industries under the Autonomous Surveillance Tower program.

The request for proposals in December said that CBP would award up to three indefinite-delivery, indefinite-quantity contracts that an 18-month baser period, and four option periods for a total potential performance period of up to 14 years.

https://www.defensedaily.com/cbp-awards-new-surveillance-tower-contracts-to-atsc-gd-elbit/homeland-security/

< https://www.atscva.com>

Advanced Technology Systems Company < https://www.atscva.com/>

CONTACT US ➤

NEWS

- ATSC Delivering Advanced Expeditionary Mobile Tactical Target Acquisition Systems (MTTAS) To US Army For EUCOM Theater

---

- **ATSC Completes U.S. Government Acceptance Testing for Integrated Fixed Tower Kits and Mobile Border Surveillance Vehicle on a CENTCOM Border Security Program**

ATSC Receives Task Order 3 As Part Of The SSS Program Of Record ($193M IDIQ) From The United States Army

Advanced Technology Systems Company (ATSC) is pleased to announce the award of Task Order 3 under the Army's Security Surveillance System (SSS) Program of Record. To this date, seven SSS systems have successfully passed Government Acceptance Testing, which demonstrates ATSC's commitment to delivering high performance solutions for critical defense needs. Task Order 3 continues the production of additional SSS units, while continuously strengthening our partnership with the U.S. Army and supporting their mission-critical surveillance requirements. ATSC remains committed to ensuring our nation's warfighters are supplied with the necessary tools and capabilities addressing our nation's most pressing and complex security needs.

> **"I am very proud of our team for their hard work and dedication to continuous improvement of these important security systems for our Armed Forces. We are grateful for the trust placed in us and we look forward to the delivery of these security systems in support of existing and emerging security requirements."**
>
> says Paul Debs, President, ATSC.

▲ US Department of Defense (DoD) Awards ATSC Multi-Million Dollar Contract to Deliver Integrated Fixed Towers (IFT) for Security Cooperation Partner

August 21, 2024- Advanced Technology Systems Company (ATSC) is pleased to announce that it has been awarded a contract to deliver 36 Integrated Fixed Towers (IFTs) under its current Mobile Surveillance Sensor Security (MS3) System Phase II program. This new award directly complements and augments ATSC's existing and future fielded mobile and relocatable border surveillance systems. ATSC's family of systems' continued success further reinforces its position as a trusted and leading provider of integrated border, maritime, and critical infrastructure security and persistent surveillance.

ATSC's IFTs monitor and control multi-domain boundaries with the best in-class hardware and software, including Integrated Command & Control (C2) while monitoring, collecting, analyzing and disseminating actionable intelligence & operational data. As a result, ATSC's integrated systems provide a real time common operating picture (COP) delivering situational awareness from the tactical edge to local, regional, and national levels of command.

"ATSC could not be prouder to continue to provide mission critical systems and solutions through the enduring trust and confidence of our customers. In today's ever-evolving global security climate, ATSC continues to be a proven "go-to" leader in solving our clients' most pressing requirements," states Paul Debs, President, ATSC, McLean, Virginia.

▶ ATSC Supports JCD Counter Swarm Event At Yuma Proving Grounds

---

▲ Advanced Technology Systems Company Expands AI-Powered Border Surveillance Tower Technology

ATSC's integrated autonomous surveillance towers protect over 26,000km of border perimeters globally. The company's autonomous and highly-customizable systems are built for long range protection, scalability, and affordability.

McLean, VA – For over two decades, Advanced Technology Systems Company < https://www.atscva.com/> (ATSC) has been a trusted partner to the Department of Defense, Department of Homeland Security, and security cooperation partner nations with their development, deployment, and support of autonomous surveillance towers protecting highly contested borders in numerous countries. ATSC's nationwide border security solutions are upgraded with the latest artificial intelligence software and customizable sensor packages to help track people, vehicles, drones, and other "objects of interest" at extended range.

"Taking feedback from deployed systems, front line operators, and government experts, we have upgraded our cutting-edge surveillance towers and force protection systems with advanced technologies to serve as a force multiplier for servicemen and servicewomen managing critical national security missions," explained Habib Debs, Chairman and CEO of ATSC.

ATSC has been an under-the-radar Prime Contractor the past two decades securing over $650M in U.S. and allied Government contracts without publicity of the achievements. The company successfully secured highly-competed programs critical to national security over traditional prime defense contractors and well-funded venture backed companies by fusing intuitive software with the latest hardware advancements, and at prices that governments can affordably scale.

"Our company employs the most impassioned veterans, technologists, and product strategists around the world to bring the most operationally-effective and future-proofed force protection and border tower solutions to military personnel and first responders – at a fair price. We are laser-focused on delivering disproportionate value for the most price competitive to give our customers an advantage," said Paul Debs, President of ATSC.

ATSC's Next Generation Tower Systems< https://www.atscva.com/capabilities/> are designed to autonomously detect, classify, track, and defeat "objects of interest" using state-of-the-art artificial intelligence, sensor fusion, and long-range advanced hardware. Built from the ground up to be highly modular and configurable to

evolving customer requirements, ATSC's systems are interoperable with over 150 different sensors and effectors.

The company's specialization in fusion of combat-proven radar, optics, electronic warfare sensors, networked communication systems, and kinetic/non-kinetic efforts into an intuitive user display gives military, government, and commercial customers access to purpose-built and proven solutions < https://www.atscva.com/products/> that safely monitor and protect borders and critical infrastructure.

To learn more about ATSC's integrated border surveillance and force protection solutions, contact info@atscva.com.

ABOUT ATSC:
Advanced Technology Systems Company < https://www.atscva.com/products/> is a private, high growth technology company that builds cutting-edge security solutions for military, government, and commercial customers. ATSC solutions help customers make better, smarter, faster decisions that save lives. The company's technology autonomously protects over 26,000km of highly-contested borders and is continuously adapting to latest emerging threats facing servicemen and servicewomen on the front lines. ATSC's technology is trusted by dozens of customers including the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Customs and Border Protection, and international military allies. Visit www.atscva.com < http://www.atscva.com> to learn more.

▸ Advanced Technology Systems Company's (ATSC) Mobile Border Surveillance Vehicles (MBSV)

Dr. Bruce Jette Joins the ATSC Board of Advisors

Friday, November 17, 2023

DHS CBP- Award ATSC $1.8B IDIQ to secure the entire USA border with Integrated Surveillance Towers (IST) Consolidated Tower & Surveillance Equipment (CTSE)

McLean, Virginia, September 7, 2023 – The US Customs and Border Protection (CBP) announced today the award of CTSE $1.8B IDIQ and DO#1 $23,421,877.51 (#70B02C23D00000024) to Advanced Technology Systems Company (ATSC), Mclean, VA to support the consolidation of its current and future border and maritime security surveillance towers.

The IST Program will use the CTSE IDIQ contracts over 14 years of total performance to acquire medium and long-range surveillance towers. These surveillance towers will be comprised of multiple subsystems that allow U.S. Border Patrol Agents to continuously detect, identify, classify, and track Items of Interest (IoI) 24 hours a day, seven days a week within each tower system's area of coverage under typical operating conditions found along the southern and northern borders. Each CTSE surveillance tower will be customized to the threat and operational/ environmental conditions of the Border Patrol Station Area of Responsibility (AoR) in which they will be deployed. CTSE consists of the following subsystems: Tower subsystem, Power subsystem, Instrumentation subsystem, and Communications subsystem. The IST Program will acquire approximately 277 new IST towers in 53 separate USBP AoRs and upgrade approximately 191 legacy surveillance towers in 31 separate AoRs.

"We are honored to have received this award in support of the Department of Homeland Security and Customs and Border Protection's mission requirements. We look forward to the execution and delivery of ATSC systems aimed at supporting DHS/CBP efforts to improve security and operational control with leading, proven integrated technologies" said Paul Debs, President ATSC."

Wednesday, 15 September, 2021

ATSC Awarded Third Contract in the Gulf Region for a Mobile Border Intelligence, Surveillance and Reconnaissance System

McLean, Virginia, 15 September 2021 – The US Army Program Executive Office for Command, Control and Communications – Tactical (PEO C3T) announced that Advanced Technology Systems Company (ATSC) has been awarded a single award contract under the GTACS II $5.1B IDIQ. ATSC successfully executed Phases 1 and 2 of the Border Surveillance programs and have proven to be a reliable partner. ATSC will design, build, and install a Phase III Mobile Border Intelligence, Surveillance, and Reconnaissance System with a Command and Control center in the Gulf region.

ATSC's CEO Habib Debs commented, "This awarded Task Order under GTACS II IDIQ is the direct result of our Team's outstanding performance and our innovative Mobile Border Command, Control, and Surveillance Solution."

Tuesday, 14 September, 2021

ATSC Awarded Navy C4I Integrated International Solutions (CIIS) Task Order in Morocco

McLean, VA (14 September 2021) – NAVWAR announced Advanced Technology Systems Company (ATSC) has been awarded a competitive bid task order under the Navy C4I Integrated International Solutions (CIIS) IDIQ for a Microwave Transmission Network in Morocco. This award is through the PEO C4I – PMW 740 – Naval Information Warfare Systems Command, San Diego, California.

ATSC's CEO Habib Debs commented, "We are very proud of our team's innovation and demonstrated capability as we continue to expand our C4ISR offerings in this strategic region".

Exhibit C

The present invention comprehends a chemical/biological/radiological/ nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as:

- Product grouping 1 (storage & transportation)
- Product grouping 2 (sensors)
- Product grouping 3 (detector case; modified and adapted)
- Product grouping 4 (monitoring & communication devices)
- Product grouping 5 (communication methods)
- Product grouping 6 (biometrics)
- Product grouping 7 (authorized person)

"WHY" WAS THE SMARTPHONE INVENTED?

BY LARRY GOLDEN

THE GOVERNMENT WAS GIVEN NOTICE OF THREE ECONOMIC STIMULUS AND TERRORIST PREVENTION PACKAGES: "THE SAFERACK PROJECT", "THE V-TECTION PROJECT", AND THE ANTI-TERRORISM PRODUCT GROUPING (ATPG) PROJECT:

Six months after the DHS was established on Nov. 25, 2002, Petitioner receive a response letter on May 21, 2003 from the Honorable Senator Fritz Hollings: "I have contacted the Department of Justice and the Department of Homeland Security to try to be of assistance"; on June 3, 2003 from the Office of the Vice President, Dick Cheney: "[y]our correspondence has been forwarded to the Department of Homeland Security for review. You will hear back directly from the Department"; on October 1, 2003 from the Honorable Senator Fritz Hollings: "[t]hank

you for contacting me regarding your difficulty with receiving a response from the Department of Homeland Security"; on October 21, 2003 from the Honorable Senator Lindsey Graham: "I have contacted the Department of Homeland Security on your behalf. I have asked that they review your request and respond directly to you"; on June 20, 2005 from the Office of the President, George Bush: "[t]hank you for your letter regarding homeland security technology procurement. Please know I have forwarded it to the Department of Homeland Security for review and response'. (STATUS REPORT: CD of Petitioner's Discovery Documents: CFC Case No. 13-307C; Dkt. No. 101; filed 02/17/2017). Also, copies of the letters can be found on my website: atpg-tech.com; click on *Larry Golden v. The United States.*

ADDITIONAL NOTICES GIVEN THE UNITED STATES

I. 2006: DoD/DARPA/SPO; BAA06-02; A.1.4 Defense against Chemical Biological Radiological Weapons. Abstract for Review to the Attention of Deputy Director Brian Pierce, Dr. Wayne Bryden, Mr. Thomas P. McCreery

II. 2006: HSARPA/SBIR; 1.1 DHS S&T TOPICS; SBIR/STTR TOPIC NUMBER: H-SB06.2-001; TITLE: SYSTEM FOR DESIGNING AND EVALUATING CHEMICAL OR BIOLOGICAL AGENT SENSOR NETWORKS. Abstract for Review to the Attention of: Mr. Mike McLoughlin

III. 2006: HSARPA/SBIR; 1.1 DHS S&T TOPICS; SBIR/STTR TOPIC NUMBER: H-SB06.2-003; TITLE: ADVANCED UNATTENDED GROUND SENSOR (UGS) TECHNOLOGIES. Abstract for Review to the Attention of: Ms. Leslee Shumway

IV. 2006: SBIR/STTR, SWIFT Tour September, 2006; Topic: Ten federal agencies collaborate to sponsor the 2006 SWIFT Tour; Executive Summary submitted to each Federal agency participating in the SWIFT Tour included NIH, DOT, NSF, DOE, Navy, Air Force, Army, DARPA, DoD, Chem-Bio Defense, NASA, and the DHS. Deborah Akwei at (202) 889-5064.

V. 2006: DHS/HSARPA/SBIR Science and Technology (S&T) Directorate Topic: High risk, high payoff R&D initiatives Executive Summary/Proposal submitted by E-mail correspondence to: Ms. Elissa (Lisa) Sobolewski; DHS/SBIR Program Manager

VI. 2007: DHS; S&T Directorate Borders and Maritime Division Topic: "White Paper" Submission for SAFECON (BAA07-02A); RFI Submitted to the attention of: Margo L. "Margo" Graves; Team Lead/ Contracting Officer

VII. 2007: U.S. Army/ECBC; Topic: ECBC agreed to develop chemical, biological, and explosives detectors, under the SAFECON BAA. Collaborative Agreements with: Daniel M. Nowak; Program Manager. Contact: 410-436-5631; daniel.nowak@us.army.mil. Dr. Augustus W. Fountain III; Chief Scientist. Contact: 410-436-0683; augustus.w.fountain@us.army.mil

VIII. 2007: Senate Committee on Homeland Security and Governmental Affairs. Topic: Container Security: "White Paper" Submission for DHS; SAFECON Project; RFI Letter sent to the Attention of: Joe Lieberman; Chairman Senate Committee on Homeland Security and Governmental Affairs, 340 Dirksen Senate Office Building, Washington, D.C. 20510

IX. 2007: US Naval Research Laboratory (NRL); Topic: Biochemical, and logistical preparations to integrate a biosensor with an appropriate air collector. Collaborative Agreements with: Chris R. Taitt; Program Manager. Contact: 202-404-4208; chris.taitt@nrl.navy.mil; Paul T. Charles; Contact person. Contact: 202-404-6064; paul.charles@nrl.navy.mil

X. 2007: DOE/ORNL Topic: Oak Ridge National Laboratory agreed to develop Chemical, Explosive, Radiological, and Nuclear detectors. Collaborative Agreements with: Blair Ross; Program Manager Contact: 865-576-1034; rossb@ornl.gov. Richard L. Stouder; Contact Person. Contact: 865-574-3053; stouderrl@ornl.gov

XI. 2007: DHS; S&T Directorate Office of Procurement Operations. Topic: "White Paper" Submission for *"CELL-ALL Ubiquitous Biological and Chemical Sensing"* (BAA07-10); RFP. Submitted to the attention of: Margo L. "Margo" Graves; Team Lead/ Contracting Officer

XII. 2007: During the year 2007, several conversations were held with Jim Culbertson (On-Star); General Motors Global Process Leadership in Warren, MI; General Motors Research and Development (R&D) Center; and, General Motors Technology Portal, Silicon Valley, CA. A letter was also sent to the Chairman & CEO of General Motors, G. Richard Wagoner, informing Mr. Wagoner that the General Motors "Stolen Vehicle Slowdown System" the company announced in October, 2007, is in fact the same system I discussed with several of its employees during the year 2007. A copy of the letter written to the Chairman and CEO of General Motors:

ATPG TECHNOLOGY, LLC
Anti-Terrorism Product Grouping
Larry Golden, CEO
522 Peach Grove Place, Mauldin, SC 29662
E-mail: lgolden5605@charter.net; E-mail: atpg-tech@charter.net
Bus. 864-288-5605 / Mobile: 864-320-0012

April 14, 2008

General Motors Corporation
G. Richard Wagoner, Jr, Chairman & CEO
P.O. Box 33170
Detroit, MI 48232-5170

Dear Mr. Wagoner:

I've made several attempts to contact Representatives of GM. I talked with and forwarded information to a few Representatives of both OnStar and GM last year during the months of March and April of 2007.

I shared with them technology I had at that time "patent pending" that is designed to stop moving vehicles. I wanted OnStar and GM to collaborate with me in responding to a Government solicitation.

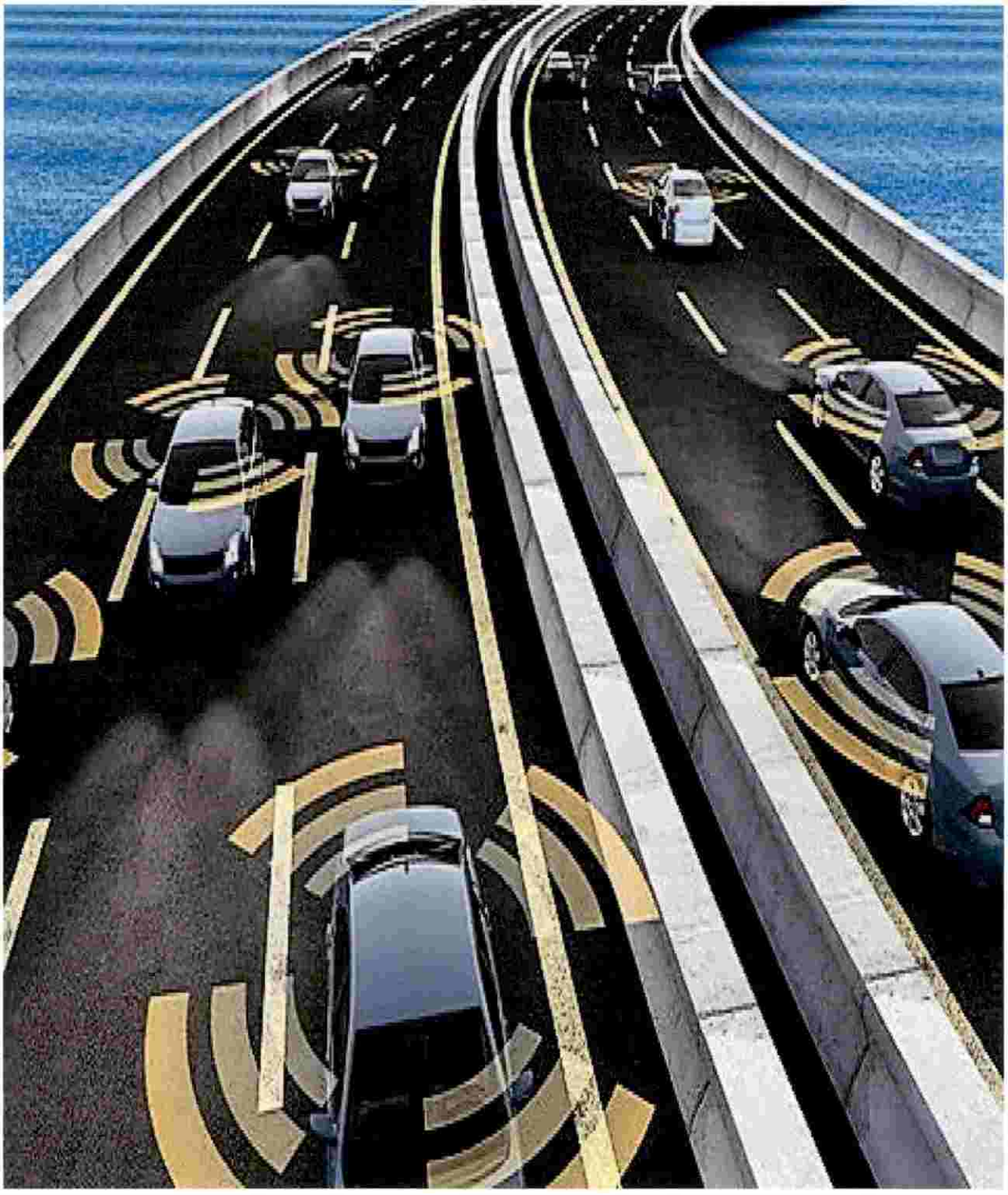
I tried again to contact OnStar and GM when you made the announcement on October 8, 2007 of having technology that will stop moving vehicles which caused your share price to move upward $4 dollars over the next 4 days (value, $2.2 billion).

I need to know if you have a patent for the technology. If you do, please send that information to me. My Patent Attorney and the PTO didn't find one. My patent application and all the claims have been allowed by the PTO.

If I don't hear back from you in a couple of days, my plans are to do a cease-and- desist for the 2 million, 2009 vehicles you have scheduled to roll out with that technology.

Thanks,
Larry Golden
Larry Golden, CEO

PREVENTING VEHICULAR TERRORIST ATTACKS WITH A STALL, STOP, VEHICLE SLOWDOWN SYSTEM



Patent Claim A vehicle adapted for receipt of a signal from a remote location to remotely control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein a user determines that the vehicle has been stolen and in response initiates a distress signal communication over a communication network that causes communication between the vehicle and the remote location and that then causes the at least one control signal to be sent from the remote location via the communication network that includes at least one of a cell phone tower and a satellite.

XIII. 2008: DHS; S&T Directorate Topic: "Read-Ahead" request made by Edward Turner prior to a face-to-face meeting at DHS. Subject matter: "Multi detection; Cell phone detection; Lock disabling; and, Stall-to-Stop "Read-Ahead" document submitted to; and face-to-face meeting held with: Edward Turner; DHS Program Manager. Doug Lane; DHS Liaison

XIV. 2008: DHS S&T LONG RANGE BROAD AGENCY ANNOUNCEMENT (BAA08-01). Topics: Cargo Container Security Device; Cell Phone Detection System; Stall-to-Stop Device "White Paper" submitted to the attention of: David Newton; Acting Division Head, Borders and Maritime Division. Contact: S&T-BordersMaritime@dhs.gov

XV. 2008: DoD/DARPA Strategic Technologies Office; (BAA) 08-10. Topic areas: 1- WMD Defense; 2- Small Unit Operations; 3- Maritime Operations; 4- Core Strategic Technologies. Submitted: A one-page "Executive Summary" via the web-based TFIMS application at http://www.tfirms.darpa.mil/baa

XVI. 2008: DHS; S&T Directorate Office of Procurement Operations "TRUST" INDUSTRY DAY. Topic: A device to detect WMD threats, Contraband; CBRNE substances contained within a maritime shipping container. Panel discussion and Proposal submission: Dave Masters; "TRUST" Program Manager

XVII. 2009: DHS; S&T Directorate Office of Procurement Operations Topic: "White Paper" Submission for "TRUST" solicitation RFI. Submitted to the attention of: Emily Graham, Contract Specialist. Contact: 202-254-5611; Emily.graham@dhs.gov

XVIII. 2009: DHS; S&T Directorate Office of Procurement Operations. Topic: Proposal Submission for *"CELL-ALL Ubiquitous Biological and Chemical Sensing"* (BAA07-10); E-mail correspondence and proposal to: Stephen Dennis, Program Manager http://cellall.webcaston.tv/home/homepage.php>

XIX. 2009: DHS; S&T Directorate. Topic: "TRUST" (BAA) 09-17: A device to detect WMD threats, Contraband; CBRNE-H substances contained within a maritime shipping container. Full proposal submission made to the attention of: Director of Innovation. Contact: BAA09-17@hq.dhs.gov

XX. 2009: DHS LEGISLATIVE AFFAIRS. Topic: Letter of support sent from the Honorable Congressman Bob Inglis office 4th District of South Carolina in reference to the "TRUST" project. Letter sent to: Eddie Gleason, DHS Director; OLA

XXI. 2010: Subcommi ttee on Emerging Threats, Cybersecurity, Science and Technology. Topic Area: CBRNE Security Meeting Request with U.S. Representative Yvette D. Clarke 1029 Longworth HOB Letter sent to the Attention of: Algene Sajery FBO / U.S. Representative Yvette D. Clarke, 1029 Longworth HOB, Washington, DC 20515

XXII. 2010: DHS; S&T Directorate (LRBAAI0-01). Borders and Maritime Division. Topic: Border Security; Maritime Security; Cargo Security. Title of "White Paper" proposal: "Integrated Systems for Border and Maritime Security". "White Paper" submitted to: SandT-BordersMaritime@dhs.gov

XXIII. 2011: DHS; S&T Directorate (LRBAA10-01).Borders and Maritime Division. Topic: Border Security; Maritime Security; Cargo Security; Title of"White Paper" proposal: "Integrated Systems for Border and Maritime Security". Response Letter from: Cherita Thomas, Associate Director/Contracting Officer. Department of Homeland Security Office of Procurement Operations Science and Technology Acquisition Division

XXIV. 2011: White House Office of Science and Technology Policy. Executive Office of the President. Topic Area: Brake Override System. Letter sent to the Attention of: Aneesh Chopra, U.S. Chief Technology Officer, 725 17th Street Room 5228, Washington, DC 20502

XXV. 2011: Larry Golden's written Testimony Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package.* Prepared for: The Honorable Aneesh Chopra U.S. Chief Technology Officer White House Office of Science and Technology Policy Executive Office of the President

XXVI. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package.* Prepared for: The Honorable David L. Strickland Administrator National Highway Traffic Safety Administration

XXVII. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package.* Prepared for: Committee on Energy and Commerce Subcommittee on Oversight and Investigations U.S. House of Representatives

XXVIII. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package.* Prepared for: The Honorable Trey Gowdy S.C. Representative; District Number 4. U.S. House of Representatives

XXIX. 2011: Larry Golden's written Testimony. Topics: *Mandate for brake override systems; Dual-use technology; Economic stimulus package.* Prepared for: The Honorable Nikki Haley, Governor S.C. Office of the Governor

XXX. 2013: Secretary's Office of DHS. Submissions made to: Ms. Janet Napolitano, Secretary of DHS. Mr. Ivan K. Fong, General Counsel of DHS

BORDER SECURITY

SBInet was a program initiated in 2006, created under U.S. Customs and Border Protection to design a new integrated system of personnel, infrastructure, technology, and rapid response to secure the northern and southern land borders of the U.S. DHS decided to have development of SBInet managed by a single private contractor.

On September 21, 2006 DHS announced the award of the SBInet contract to Boeing. Boeing, holding the primary contract, subcontracted many portions of the design, development, implementation, and maintenance of the program, while Boeing handled the majority of the management aspects.

SBInet was controlled by an indefinite delivery/indefinite quantity contract extending through September 30, 2009, with three one-year option periods. The only commitment DHS

made was to pay for a 28-mile pilot section of SBInet in the Tucson sector of the Arizona-Mexico border. The cost of the pilot section was estimated at $67 million. The value of Boeing's three-year contract to build SBInet across both the northern and southern borders was estimated by various sources at various times to be between $2 billion and $8 billion. The technology included:

Tower system: Towers were meant to be set up along the border, with varying surveillance and communications equipment. Towers were slated to include radar, long-range cameras, broadband wireless access points, thermal imaging capabilities, ground sensors, and motion detectors.

Command centers: All of the information received by sensors were meant to go to command centers, where a "common operating picture" would have been compiled and shared with other agencies. The common operating picture would have appeared on computer screens as a geospatial map, where border entries are tracked in real time. Command center personnel were supposed to be able to click on a given entry, view the entry, and assess the threat using the long-range cameras on the towers.

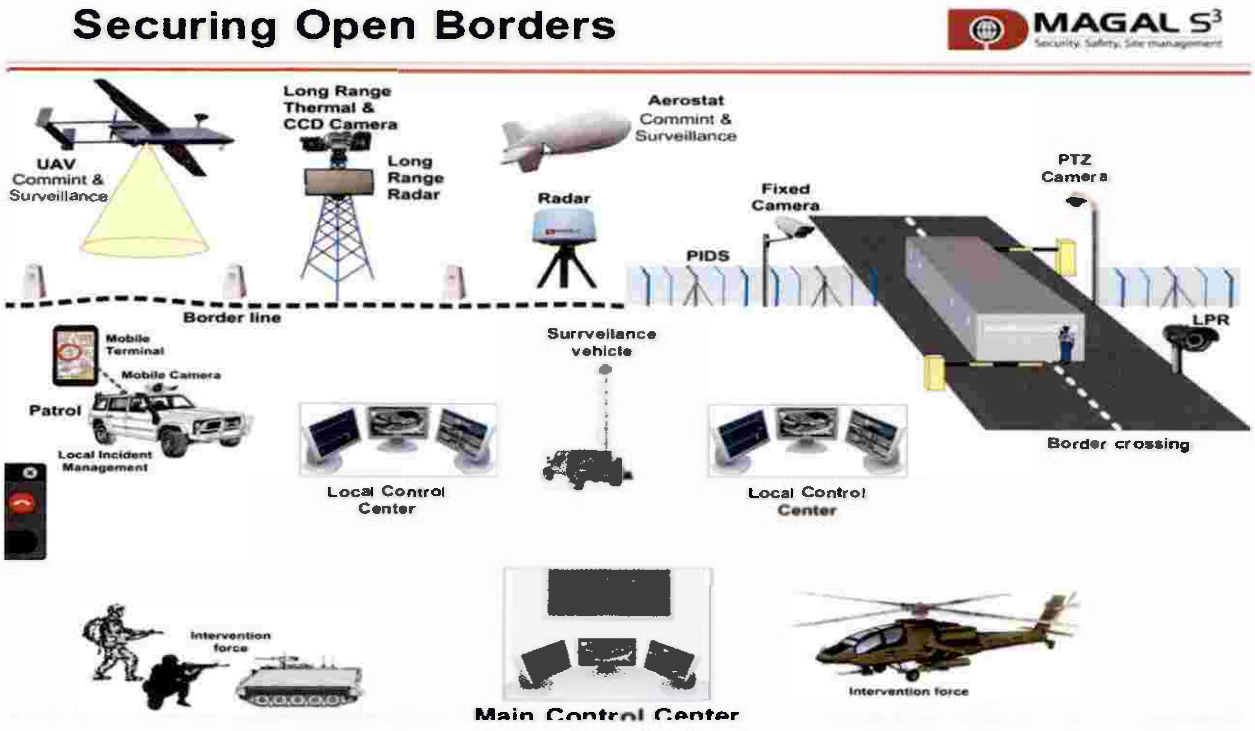
Border Patrol response: Border Patrol agents were meant to carry PDAs with GPS capabilities, to allow the command center to track the location of agents prohibiting illegal entries and watch the encounter in real time on the common operating picture. Additionally, the PDAs were supposed to have advanced finger print identification technology, to allow Border Patrol agents to identify an individual at the prohibition site immediately and the ability to view and control tower cameras from their PDA. In addition, Border Patrol agents will be given laptops in the patrol car.

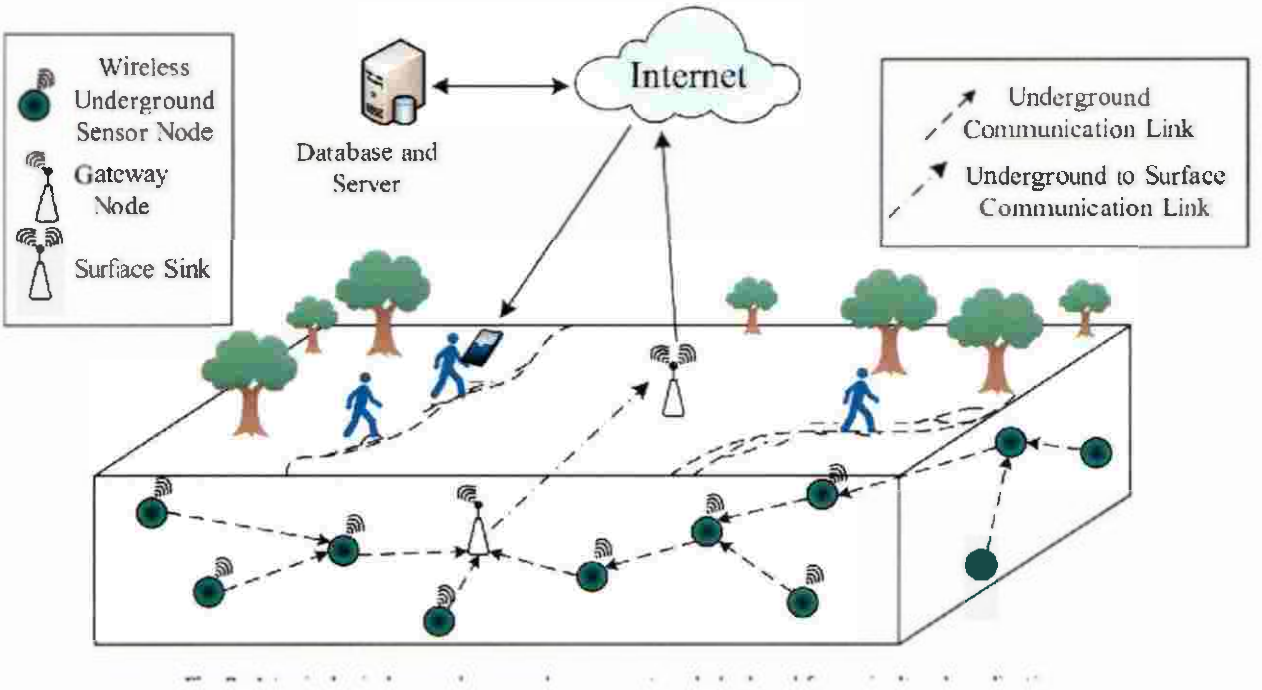
Airborne sensors: Airborne sensors on unmanned aerial vehicles (UAVs) were meant to fill in gaps in the "virtual fence" in remote areas where building and maintaining towers was impractical.

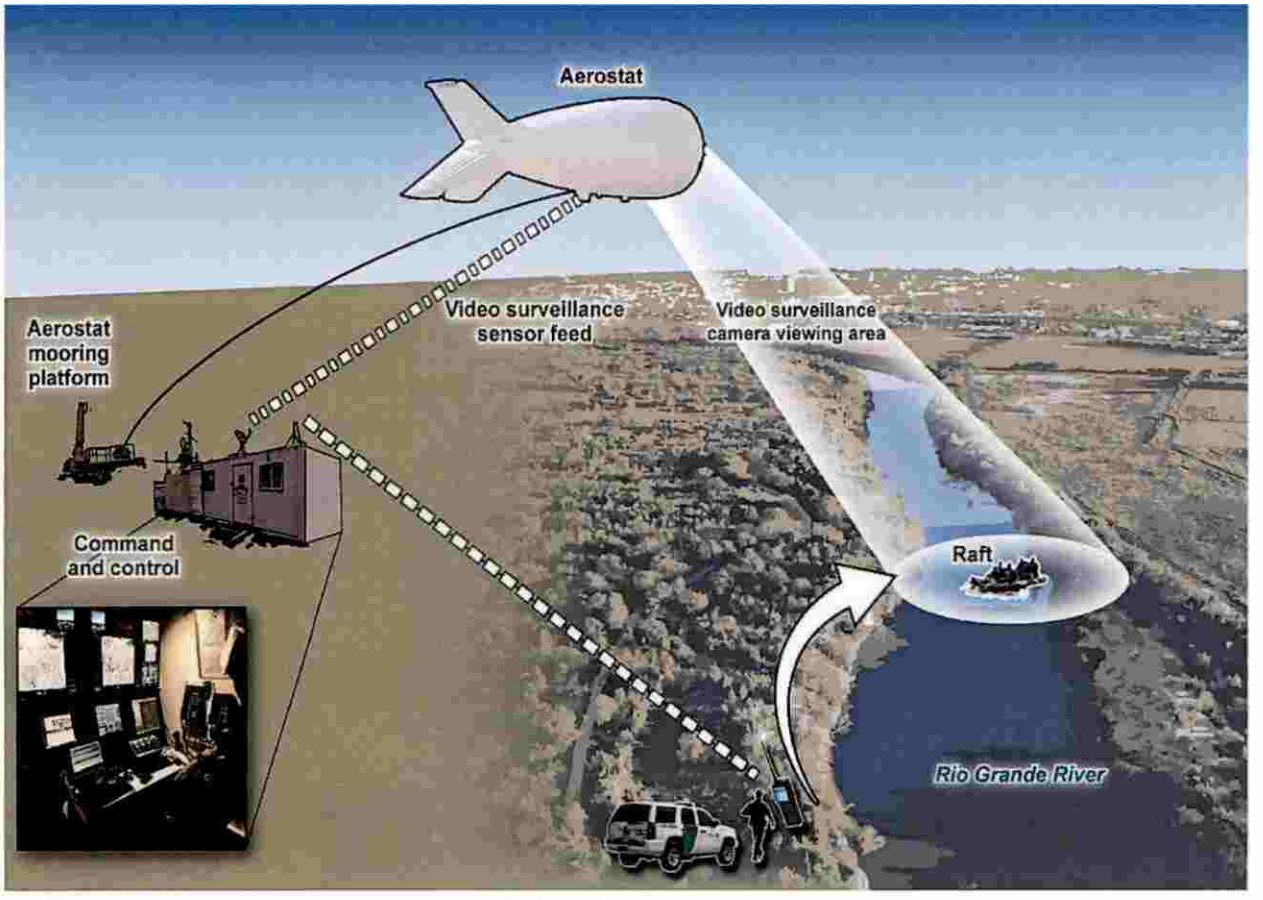
Janice Kephart of the Center for Immigration Studies defended SBINet, writing, "SBInet is still operational where it was deployed, despite the widespread notion that the light switch was turned off. She stated, "the reason SBInet is still operating is because it works".

DHS Secretary Janet Napolitano ordered an assessment of the project in January 2010 and in March 2010 froze additional funding. On Jan. 14, 2011, DHS said it would redirect

funding originally intended for SBInet—including fiscal 2011 SBInet funds—to the new border security technology effort.







Source: GAO analysis of U.S. Customs and Border Protection (CBP) information; CBP (photos). | GAO-17-152

Patent Claim A multi sensor detection system capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities vulnerable to terrorist activity that can be integrated with and interconnected to watchtowers to form a network, comprising:

at least one of an integrated watchtower, a fixed watchtower, a surveillance watchtower, a watchtower capable of scanning, a watchtower capable of monitoring, a watchtower equipped with sensors or a watchtower interconnected to a central monitoring terminal for sending signals thereto and receiving signals therefrom;

wherein the at least one watchtower is equipped with a remote video surveillance camera that provides at least one night vision means of surveillance or an infrared human detection means of surveillance capability and is integrated into a watchtower's remotely controlled system that can monitor, detect, track, and identify humans;

a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop personal computer (PC), a notebook personal computer (PC), a laptop, a satellite phone, a smart phone, a cell phone, a Universal Mobile Telecommunications System (UMTS) phone, a personal digital assistant (PDA), a liquid crystal display (LCD) monitor, a satellite, or a handheld, interconnected to a monitoring equipment for sending signals thereto and receiving signals therefrom;

a communication method of at least one of a Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), or central processing unit (CPU), used to interconnect the communication device to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a plurality of sensors for detecting or sensing humans that is at least one of a chemical human sensor, biological human sensor, radiological human sensor, infrared human detector, motion human detector, or image human detector, interconnected to or disposed within the multi-sensor detection system for sending signals thereto and receiving signals therefrom;

a mobile multi-sensor detection device that is at least one of a ground surveillance sensor,

a surveillance radar sensor, a surveillance camera, or a stand-alone surveillance scanner, that is mounted in, on, or upon at least one of a car, a truck, a camper, a bus, a van, an unmanned aerial vehicle (UAV), an unmanned ground vehicle (UGV), or a utility vehicle, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a hand-held multi-sensor detection device that is capable of at least one of thermal imaging or infrared imaging for monitoring, detecting, tracking and identifying humans, that is controlled or operated by at least one authorized person who is an owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, or monitoring site and terminal personnel, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, wherein the authorized person manually initiates the signal to the monitoring equipment to alert upon the monitoring, detecting, tracking and identifying of the human;

whereupon, detection by the mobile multi-sensor detection device causes an automatic signal transmission to be sent to, or received from, any products in product grouping categories of storage and transportation, sensors, detector case; modified and adapted, monitoring and communication devices, communication methods, biometrics;

whereupon, detection of an unauthorized vehicle, an unauthorized driver or operator of a vehicle or mobile unit, a signal is sent from the communication device to the vehicle or mobile unit to stop, stall or slowdown the vehicle;

wherein, a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop PC, a notebook PC, a laptop, a satellite phone, a smart phone, a cell phone, a UMTS phone, a PDA, a LCD monitor, a satellite, or a handheld, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, comprising a lock disabling mechanism that is able to engage (lock), and disengage (unlock) and disable (make unavailable) after a specific number of tries.

Patent Claim The multi sensor detection system of claim 1, capable of identifying,

monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities, further includes the identifying, monitoring, and detecting of terrorist, that is at least one of an illegal, radical, fanatic, activist, revolutionist or rebel.

Patent Claim The multi-sensor detection system of claim 1, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The multi-sensor detection system of claim 1, further includes a navigation system adapted for communication with at least one of the surveillance watchtowers.

Patent Claim The multi-sensor detection system of claim 1, capable of forming a wired or wireless sensor network.

Patent Claim The multi-sensor detection system of claim 1, capable of transmitting identification data, location data, power source data, and sensor data.

Patent Claim The multi-sensor detection system of claim 1, capable of being embedded into; placed in, on, or adjacent to at least one of the products in the product grouping categories or an area targeted for monitoring.

Patent Claim The multi-sensor detection system of claim 1, capable of sending signals thereto and receiving signals therefrom to engage (lock), disengage (unlock) and disable (make unavailable) a lock after a specific number of tries that is interconnected to the multi sensor detection system or monitoring equipment.

Patent Claim The multi-sensor detection system of claim 1, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The multi-sensor detection system of claim 1, interconnected with a camera to

view the environment in real-time or to store the data for transmission and review at a later time.

Patent Claim The multi-sensor detection system of claim 1, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

UNMANNED AERIAL VEHICLE (UAV) / UNMANNED GROUND VEHICLE (UGV)

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.

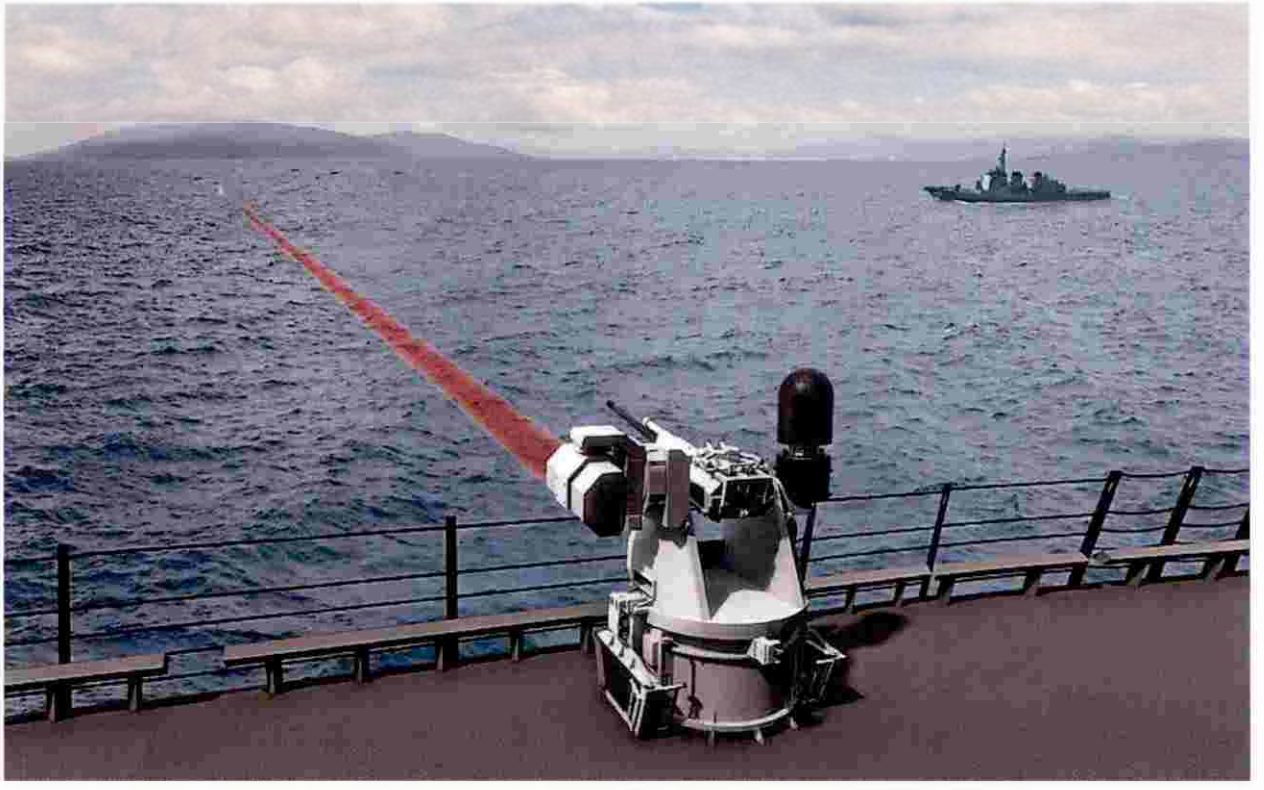
Patent Claim The multi-sensor detection and automatic/mechanical lock disabler system of claim 12 wherein the cell phone detector case includes telecommunication and radio communication means that are interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships, UAVs, UGVs, and airplanes.

Patent Claim The communication device of claim 11 wherein the communication device includes telecommunication, telematics, long and short range radio frequency communication

means that are interactive with any type of motive vehicle that includes, but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships, UAVs, UGVs, and airplanes.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case includes telecommunication, telematics, long and short range radio frequency communication means that are interactive with any type of motive vehicle comprising a car, truck, van, SUV, train, subway, boat, ship, UAV, UGV, or airplane.

ELECTROMAGNET PULSE, ELECTROSTATIC DISCHARGE, MICROWAVE BEAM OR RADIO FREQUENCY TO STALL, STOP, OR SLOW-DOWN A VEHICLE



Patent Claim A vehicle adapted for receipt of a signal from a remote location to control the vehicle's stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein the at least one control signal is sent due to unauthorized use of the vehicle, and wherein an originating first signal that eventually causes the at least one control signal to be sent is generated upon initial verification of the unauthorized use of the vehicle;

at least one mobile, portable, or fixed device capable of sending the at least one control signal from the remote location that is of electromagnet pulse, electrostatic discharge, microwave beam or radio frequency, to disable the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and horsepower of the motor.

AUTONOMOUS VEHICLE EQUIPPED WITH AN ELECTROMAGNET PULSE, ELECTROSTATIC DISCHARGE, MICROWAVE BEAM OR RADIO FREQUENCY TO STALL, STOP, OR SLOW-DOWN A VEHICLE

Patent Claim A vehicle adapted for receipt of a signal from a pre-programmed automated system to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein the receivers, the computer system, and the electrical system are part of at least one pre-programmed operating system of unintended acceleration, pre-crash, reverse acceleration, stabilization, lane departure, cruise control, driverless vehicle, and chemical biological radiological nuclear explosive (CBRNE) detection;

wherein the control signal to activate the stall-to-stop or vehicle slowdown is not remote from the vehicle and the signal to activate is initiated when at least one of the vehicle's operating systems for monitoring the vehicle's condition exceeds a pre-programmed vehicle operating system parameter.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, pre-programmed automated system further including a cellular communication device adapted for communication with at least one cell phone tower; further including, at least one satellite connection capable of communicating with the pre-programmed automated system; further including, at least one modem connection for short and long range radio frequency transmissions with the pre-programmed automated system.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system

and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is an in-vehicle notification warning of: crash, vehicle parking, speeding; driving too fast for conditions; construction zone; school zone; accident ahead; brake failure; acceleration/deceleration failure; acceleration/deceleration cruise control.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when the vehicle is in forward movement, backward or reverse movement, side movement, cruise control movement, or lane departure movement or when the vehicle moves outside a designated perimeter or zone.

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is a detection of a bomb, weapon of mass destruction, chemical or biological agents, located in, on, or adjacent to a vehicle.

MARITIME CARGO CONTAINER DETECTION DEVICE

Patent Claim A maritime cargo container multi-sensor detection system for monitoring products and for detecting at least one explosive, nuclear, contraband, chemical, human, biological, or radiological agents so that terrorist activity can be prevented, comprising:

a plurality of sensors for detecting the at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and capable of being disposed within a multi-sensor detection device;

monitoring equipment located at a determinate site that is remote from the maritime cargo container and not in contact with the maritime cargo container, to include, but is not limited to at least one of computers, laptops, notebooks, PCs, handhelds, readers, cell phones, PDAs or smart phones for the receipt and transmission of signals therebetween;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

at least one satellite capable of transmitting signals to the monitoring equipment and receiving signals from the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication with the maritime cargo container multi sensor detection device;

at least one modem for short and/or long range radio frequency communication with the maritime cargo container multi sensor detection device;

at least one interface for establishing a remote, global communications and tracking network that works with the maritime cargo container multi-sensor detection device;

at least one internet connection capable of communication between the maritime cargo container multi sensor detection device and the monitoring equipment;

whereupon a signal sent from a maritime cargo container multi sensor detection device to a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes the transmitting of location data and sensor data.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of forming a wired or wireless sensor network.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of forming a mesh network for redundancy.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of transmitting identification data, location data, power source data, and sensor data.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, wherein the power source is electrical, battery, solar, or a combination thereof.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of being embedded into; placed in, on, or adjacent to a product or area targeted for monitoring.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of sending signals thereto and receiving signals therefrom to lock, disable a lock, enable a lock, or unlock a lock that is interconnected to the multi sensor detection device and monitoring equipment.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, capable of transmitting biometric and authentication data include, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, interconnected with a camera to view the environment in real-time or to store the data for transmission and review at a later time.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56,

interconnected with a camera; light and video sensors to allow the user to view the environment from a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, wherein the maritime cargo container multi-sensor detection device is capable of receiving signals and messages from, and sending signals and information to, at least one of; a remote lock, a remote communication device, a vehicle and another multi-sensor detection device.

Patent Claim The maritime cargo container multi-sensor detection system of claim 56, wherein the maritime cargo container multi-sensor detection device is capable of communicating through a physical interface.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of a unique ID number with authentication; timing/location signal; sensor status; battery condition, stored sensor messages, and can alert a remote monitor.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of monitoring and allowing transmission and propagation of containers while stacked, either afloat or ashore.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of having interfaces with environmental and security sensors and is able to interrogate and pass data from the sensors.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of capable of communicating a security alert globally through the use of radio frequency, cellular and satellite technology.

Patent Claim The maritime cargo container multi-sensor detection system of claim 68, wherein the physical interface is capable of sending signals and messages to; receiving signals

and messages from; at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation or monitoring site.

SEAPORT CRANE, HARBOR CRANE OR STRADDLE-CARRIER

Patent Claim A maritime cargo container multi-sensor detection system for monitoring and for detecting at least one explosive, nuclear, human, contraband, chemical, biological, or radiological agents and compounds so that terrorist activity can be prevented, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds;

monitoring equipment located at a determinate site that is remote from the maritime cargo container and not in contact with the maritime cargo container, that is at least one of a computer, laptop, notebook, PC, handheld, transceiver, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;

at least one of a modem for short and/or long range radio frequency, a cellular connection, a Wifi connection, a satellite connection, an interface connection, or an internet connection, interconnected to the monitoring equipment for sending signals and messages thereto and receiving signals and messages therefrom;

a maritime cargo container multi-sensor detection device that is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of loading, offloading, or transport within the seaport terminal facility;

whereupon a signal sent from the maritime cargo container multi sensor detection device to a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data.

Patent Claim The multi-sensor detection system of claim 136, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

Patent Claim The multi-sensor detection system of claim 136, capable of forming a wired or wireless sensor network.

Patent Claim The multi-sensor detection system of claim 136, capable of forming a mesh network for redundancy.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of transmitting identification data, location data, power source data, and sensor data.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, wherein the power source is electrical, battery, solar, or a combination thereof.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of, a seaport crane, a harbor crane or a straddle-carrier, capable of sending signals thereto and receiving signals therefrom to lock, disable a lock, enable a lock, or unlock a lock that is interconnected to the maritime cargo container multi sensor detection device and monitoring

equipment.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of., a seaport crane, a harbor crane or a straddle-carrier, capable of transmitting biometric and authentication data that includes, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The multi-sensor detection system of claim 136, wherein the maritime cargo container multi-sensor detection device is embedded into, placed in, on, upon or adjacent at least one of., a seaport crane, a harbor crane or a straddle-carrier, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation or a monitoring site.

A COMMUNICATING, MONITORING, DETECTING, AND CONTROLLING (CMDC) DEVICE FOR BORDER SECURITY

CMDC DEVICE/ BIOMETRIC DATA BASE FOR REGISTERING IMMIGRANTS

Patent Claim The multi-sensor detection system of claim 1, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The multi sensor detection security systems of claim 145, further including biometrics of at least one of, but not limited to fingerprints, iris, signature and voice to prevent entry or exit of unauthorized persons.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.

Patent Claim The multi-sensor detection system of claim 81, wherein the multi sensor detection device is capable of transmitting biometric and authentication data including, but is not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

Patent Claim The communication device of claim 11 wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals

CMDC DEVICE / HOME, BUILDING, AND CARGO CONTAINER LOCKS

Patent Claim Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to at least one of a home lock, a building lock, or a cargo container lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a home lock, a building lock, or a cargo container lock;

a receiver for receiving signals from at least one of a home lock, a building lock, or a cargo container lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RE) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long

range radio frequency (RF) connection, short range radio frequency (RE) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and,

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a home lock, a building lock, or a cargo container lock whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the home lock, building lock, or cargo container lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

CMDC DEVICE/ UNMANNED AERIAL, LAND, SEA VEHICLE LOCKS

Smartphone Controlled Drone Market

Patent Claim Monitoring equipment that is at least one of products grouped together by

common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal, digital assistant (PDA) or smart phone interconnected to a vehicle lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;

a receiver for receiving signals from at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RF) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and,

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock, whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the manned or unmanned aerial vehicle lock, manned or unmanned ground vehicle lock, or manned or unmanned sea vehicle lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

CMDC DEVICE/ INTERNET OF THINGS (IoTs) FOR BORDER SECURITY

Patent Claim A monitoring equipment, comprising:

at least one central processing unit (CPU);

at least one motion sensor in communication with the at least one CPU;

at least one light indicator in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

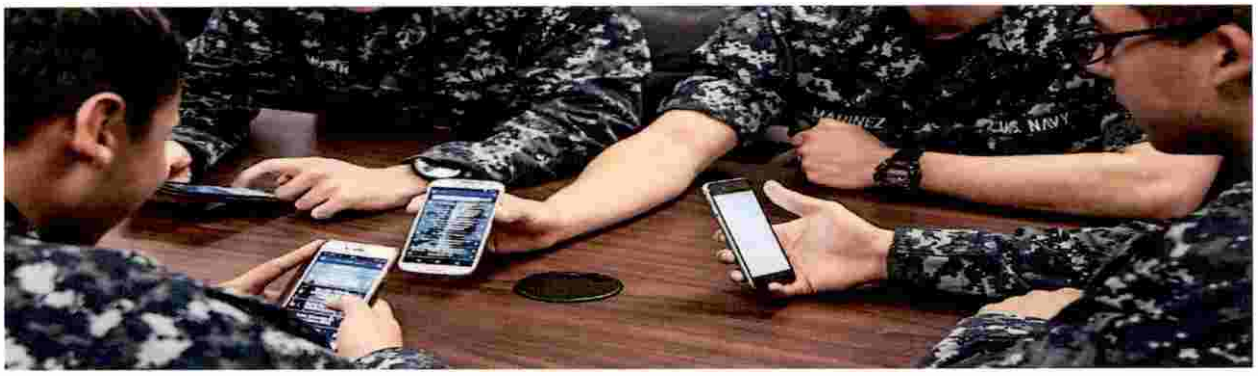
at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;

at least one or more detectors in communication with the art least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the **communication device is capable of communicating, monitoring, detecting, and controlling.**

CMDC DEVICE/ FOR MILITARY AND BORDER SECURITY PERSONNEL



Patent Claim The communication device of claim 11 wherein the communication device having products to be monitored, the devices that are monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.

CMDC DEVICE/ ENABLES (MAKE AVAILABLE) THE CMDC DEVICE AFTER A BIOMETRIC FINGERPRINT OR FACIAL AUTHENTICATION IS MADE TO THE DEVICE BY AN AUTHORIZED USER (The first smartphone with a fingerprint reader was the Motorola Atrix 4G in 2011)

Patent Claim A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that **the communication device is capable of communicating, monitoring, detecting, and controlling.**

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case are designed to be used with biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.

CMDC DEVICE/ LOCATION FOR THE CMDC DEVICE ITSELF; INTERCONNECTED TO THE MULTI SENSOR DETECTION DEVICES; THE STALL TO STOP SYSTEMS; AND, THE LOCKING MECHANISMS

Apple Location Services allows Apple and third-party apps and websites to gather and use information based on the current location of your iPhone or Apple Watch to provide a variety of location-based services. To use features such as these, you must enable Location Services on your iPhone and give your permission to each app or website before it can use your location data. Location Services uses GPS and Bluetooth (where those are available) along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your device's approximate location. Your Apple Watch may use the location of your paired iPhone if it is nearby.

If Location Services is on, your iPhone will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers in an anonymous and encrypted form to Apple, to be used for augmenting this crowd-sourced database of Wi-Fi hotspot and cell tower locations.

By enabling Apple's Location Services, location-based system services such as these will also be enabled:

- **Traffic**: If you are physically moving (for example, traveling in a car), your iPhone will periodically send GPS locations and travel speed information in an anonymous and encrypted form to Apple, to be used for augmenting a crowd-sourced road traffic database.
- **Significant Locations**: Your iPhone will keep track of places you have recently been, as well as how often and when you visited them. This data is encrypted and stored only on your device and will not be shared without your consent. It is used to provide you with personalized services, such as predictive traffic routing.
- **Location-Based Suggestions**: If you turn off Location Services for Location-based Suggestions, Apple may use the IP address of your internet connection to approximate your location by matching it to a geographic region.
- **Location-Based Alerts**: Your iPhone and Apple Watch will use your location in order to provide you with geographically-relevant alerts, such as a reminder to call someone when you get to a specific place.
- **Share My Location**: You can choose to share your current location with others, on a temporary or ongoing basis, from within certain apps such as Messages and Find My Friends.
- **HomeKit**: Your iPhone will use your location to enable accessories to turn on or off when you arrive at or leave a specific location, such as turning on your lights when you get home.
- **Emergency Calls & SOS**: When you make an emergency call, in addition to location already provided to emergency services, your iPhone will make supplementary location data available through the Enhanced Emergency Data service, where supported. In addition, triggering emergency SOS will send location to your emergency contacts at the end of the call.

Ouote from the "CellAll" Proposal submitted to the DHS in 2007, "Initially the SMD will look to the on-board GPS (if provided) to determine position. If the cell phone is equipped with a GPS the application on the cell phone will retrieve the position from its own GPS. When a GPS position cannot be determined, the position of the SMD and its user will be calculated based on a cell phone tower database, provided by the FCC and signal strength. If this does not yield a result, the Wi-Fi hotspot database will be utilized to determine SMD and user position. If all these options fail, the last known position can be augmented with the on board accelerometers to

estimate the current position which will be reported to the control centers and annotated as a last position and a possible position."

Patent Claim The communication device of claim 11 wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.

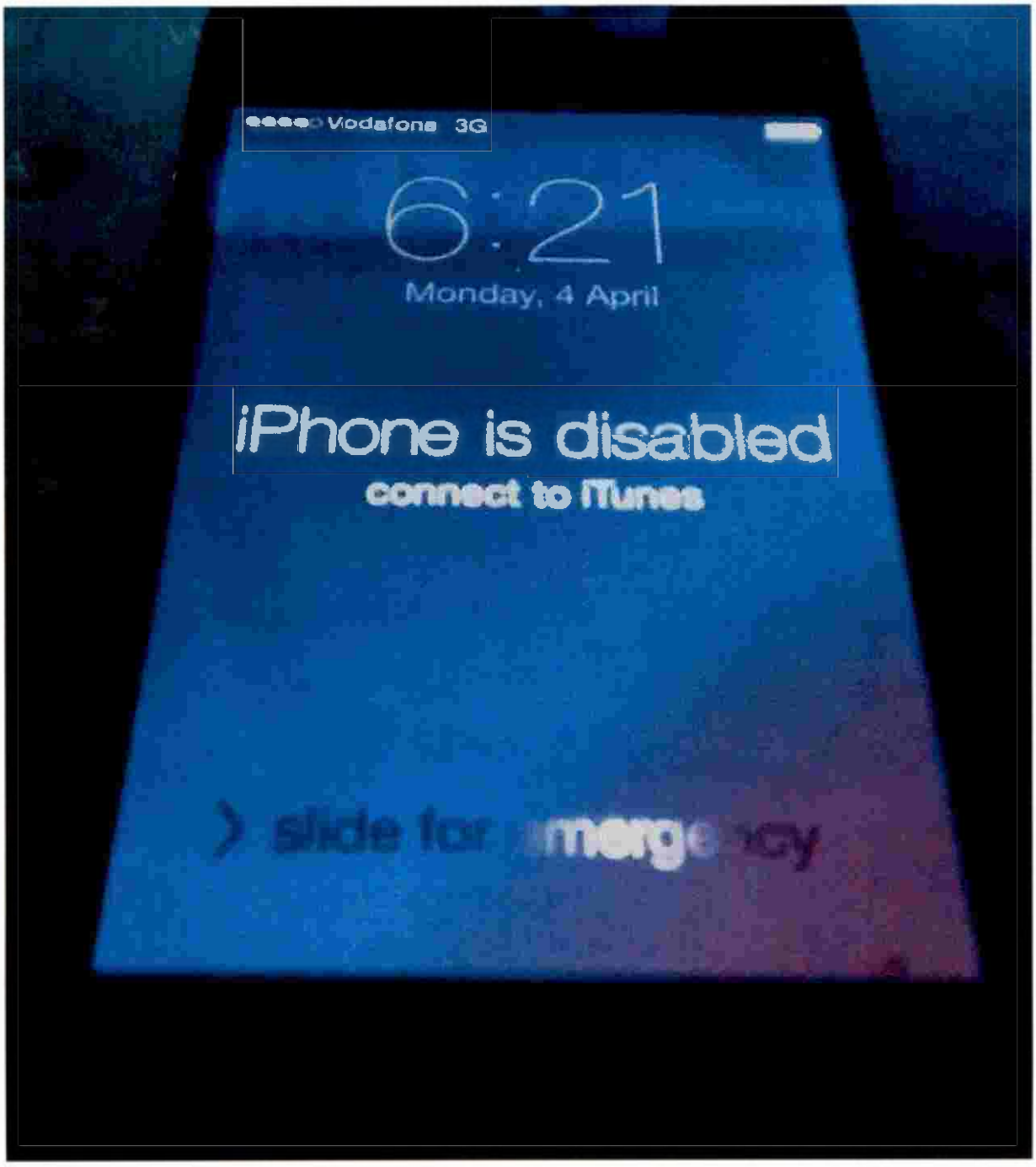
Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case have at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, or a GPS connection.

Patent Claim The multi-sensor detection system of claim 125 wherein the internal or external remote/electrical lock disabler includes at least one of: a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are interconnected to the central processing unit (cpu).

Patent Claim The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 11, wherein a communication link is present of at least one of a Wi-Fi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom monitoring equipment and a central processing unit (CPU) or a transceiver on the vehicle.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device includes at least one of; a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are capable of being interconnected to a central processing unit (cpu) of the communication device.

CMDC DEVICE/ DISABLE (MAKE UNAVAILABLE) THE CMDC DEVICE AFTER MULTIBLE FAILED ATTEMPTS TO DENY ACCESS TO THE DEVICE BY UNAUTHORIZED USERS (In 2014, Apple's "Find my iPhone" and Google's "Android Device Manager" can locate, disable, and wipe the data from phones).



Patent Claim A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that **the communication device is capable of**

communicating, monitoring, detecting, and controlling.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the product by unauthorized, untrained, and equipped individuals.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to lock, or disable the lock of the product thus preventing further contamination and denying access to the product by unauthorized, untrained, and unequipped individuals.

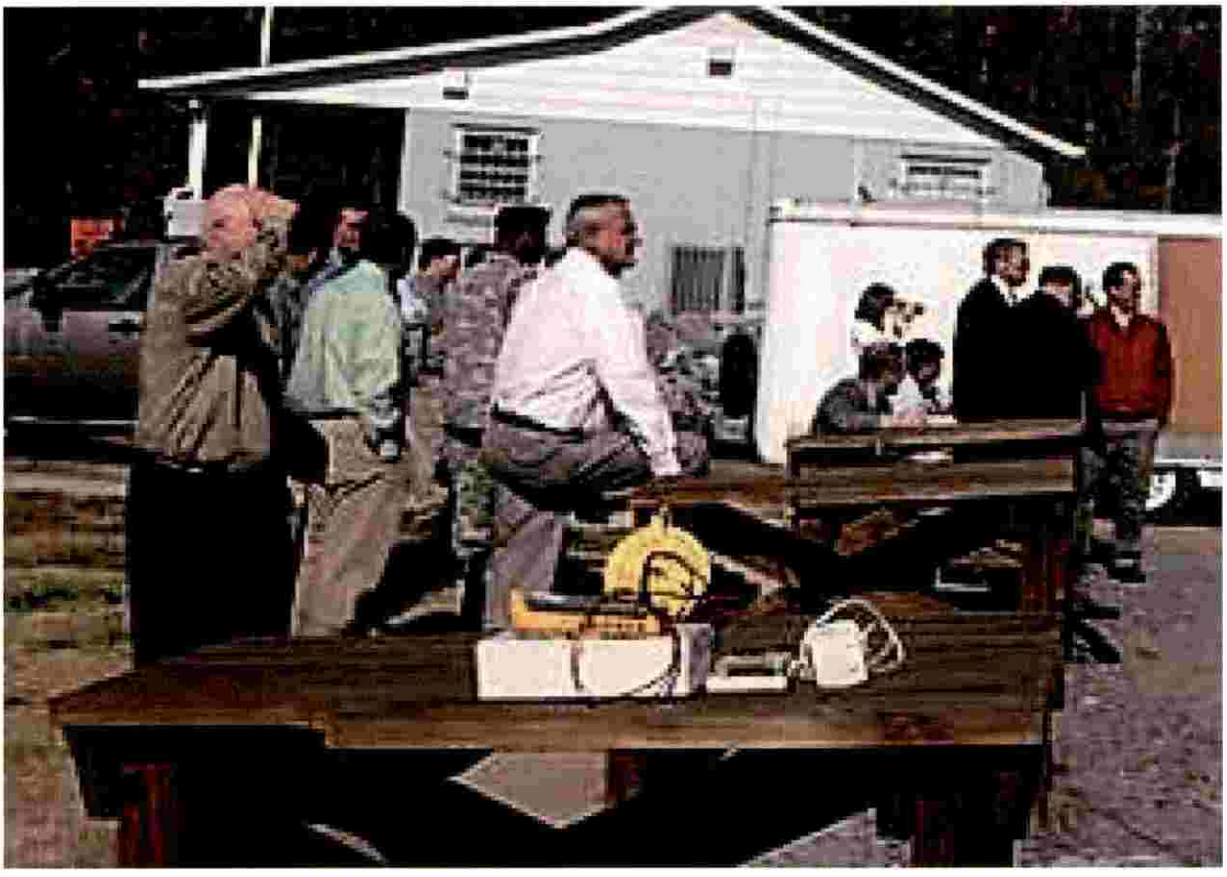
Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to unlock or enable the lock of the product thus allowing access to the product by authorized, trained, and equipped individuals.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device is designed for outside and/or inside of the products listed in the product grouping.

Patent Claim The lock disabler system of claim 33 wherein the automatic/mechanical lock disabler detection device can be used with cars, trains, airplanes, ships and any of the products listed in the product groupings.

CMDC DEVICE/ RADIO FREQUENCY NEAR FIELD COMMUNICATION (NFC); A BETTER CHOICE FOR RADIO FREQUENCY (RF) COMMUNICATION WHEN COMPARED TO RADIO FREQUENCY IDENTIFICATION (RFID)



RFID Signals can Detonate Bombs in Cargo Containers: But How Serious is the Vulnerability?

August 10, 2011 Homeland Security Today

In the fall of 2007, a handful of officials from the Department of Homeland Security (DHS) were invited to attend a live demonstration of how a bomb hidden inside a commercial cargo container could be detonated by a homemade radio frequency identification (RFID) container tracking tag operating at a frequency that was mandated by the federal government for cargo containers within US port environments.

A cargo container RFID electronic tag, or seal, contains an electronic reader that receives a port's RFID signal that prompts the container's RFID tag to transmit to port authorities' data regarding the cargo that's been encoded on its RFID tag. But as the

demonstration showed, it also can be used to close an electronic circuit when it receives a corresponding RF from a port RFID sender/receiver, thereby detonating the bomb. Indeed. In the November, 2007 test, an RF receiver tuned to pick up a required US port RFID reader frequency triggered the small explosive that had been placed inside the empty container.

What's important about the demonstration is that the homemade RF receiver was operating at a frequency that not only was mandated to be used within port environs, but also was mandated to be made public despite the fact that "the process of selecting a frequency for container security was contentious," *Homeland Security Today* was told by Powers Global Holdings, Inc. Chairman, a former FBI agent who worked with CBP on border related security issues while in Laredo, Texas.

RFID systems consist of a reader with an antenna, and a transponder (tag). There are two different RFID tags possible. Either they are active, meaning they have their own power source or they are passive. Passive tags have no own power source and have to be supplied with energy via an electromagnetic field produced by the reader.

NFC stands for Near-Field Communication. NFC is also based on the RFID protocols. The main difference to RFID is that a NFC device can act not only as a reader, but also as a tag (card emulation mode). In peer-to-peer mode, it is also possible to transfer information between two NFC devices. Because of the short read range limitations, NFC devices have to be in very close proximity - usually no more than a few centimeters. That's why NFC is often used for secure communications.

NFC is almost exclusively used for high-speed data transfer between two electronic systems, like a smartphone and a payment reader in the checkout line, or two smartphones exchanging data, for example. NFC enables bi-directional communication through dual-mode hardware, so a device can act as both a reader and a tag. For example, you can "bump" two Android phones together and exchange information using the NFC standard, or set up a secure session to exchange crypto for payment.

NFC allows communication from passive tags. For example, when you place your NFC-enabled credit card on a tap-to-pay credit card terminal, the energy from the NFC reader sends a burst of energy and excites the NFC chip in the card. At the same time the reader is verifying the card, the card is ensuring that the reader is valid. This kind of two-way processing isn't something you can do with passive RFID; when the passive reader sends out a burst of energy, the passive RFID tag can only transmit back a number.

Patent Claim A monitoring device, comprising:

at least one central processing unit (CPU);

at least one temperature sensor in communication with the at least one CPU for monitoring temperature;

at least one motion sensor in communication with the at least one CPU;

at least one viewing screen for monitoring in communication with the at least one CPU;

at least one global positioning system (GPS) connection in communication with the at least one CPU;

at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;

at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;

at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;

at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;

at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;

one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;

at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and,

at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that **the communication device is capable of communicating, monitoring, detecting, and controlling.**

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case are designed to be equipped with a radio frequency (RF) chip for the locking, disabling a lock, enabling a lock, and unlocking the locks of containers, vehicles, houses and businesses, and are capable of a two-way, bi-directional radio frequency (RF) communication link that makes the cell phone, the smart phone, and the cell

phone detector case work as a radio frequency (RF) sensors or a radio frequency (RF) transceiver.

CMDC DEVICE/ DETECTOR CASE

The Smartwatch has the same features as the cellphone detector case and the CMDC Device (i.e. smartphone) described in the Patents owned by Larry Golden.

C – Communicating: cellular, Bluetooth, Wi-Fi, GPS, NFC, E-mail, call alerts, alarms
M – Monitoring: heart rate monitor, blood pressure monitor (i.e. chem/bio monitoring)
D – Detecting: carbon monoxide, natural gas, blood oxygen, seizure (i.e. chem/bio detection)
C – Controlling: lock and unlock doors, remote vehicle controls to include engine start

Patent Claim The multi-sensor detection system of claim 81, wherein the multi sensor detector device is a multi-sensor embedded or built-in device designed for, but not limited to, at least one of a cell phone, a smart phone, a PDA, a handheld, a cell phone detector case, a smart phone detector case, a PDA case, a handheld case or another communication device.

Patent Claim The multi-sensor detection system of claim 103 wherein each cell phone detector case includes an internet connection, a GPS connection, a radio frequency (RF) connection, a recharging cradle or seat, a front side, a top, a bottom, a pair of opposed sides and a central processing unit (cpu).

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone; the smart phone; and the cell phone detector case includes standard keypad functions and more specialized system use ring tone, email, photos, and texting functions as well as viewing screens.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone, the smart phone, and the cell phone detector case includes telecommunication, telematics, long and short range radio frequency communication means that are interactive with any type of motive vehicle comprising a car, truck, van, SUV, train, subway, boat, ship, UAV, UGV, or airplane.

Patent Claim The multi-sensor detection system of claim 103 wherein the cell phone the smart phone, and the cell phone detector case are capable of sending signals to a vehicle's operating equipment systems comprising at least one of an ignition for starting and stopping, a lock for unlocking and locking, a horn for sounding; and are capable of receiving data and diagnostic information of the vehicle's operating equipment systems.

"WHO" INVENTED THE SMARTPHONE?

BY LARRY GOLDEN

BROAD AGENCY ANNOUCEMENT (BAA)

BAA07-10

CELL-ALL Ubiquitous Biological and Chemical Sensing

Published: *10/30/2007*
BAA07-10
Published: 10/30/2007

INTRODUCTION

This solicitation is a Broad Agency Announcement (BAA), as contemplated in Federal Acquisition Regulations (FAR) 6.102(d)(2) and 35.016. A formal Request for Proposal (RFP) will not be issued in this matter.

The Department of Homeland Security (DHS) Science & Technology (S&T) Directorate will not issue paper copies of this announcement. DHS S&T reserves the right to select for award and to fund all, some, or none of the full proposals received in response to this solicitation. No funding for direct reimbursement of proposal development costs will be allowed. Technical and cost proposals, or any other material, submitted in response to this BAA will not be returned.

However, depending on the markings on the proposal, DHS S&T will adhere to FAR policy on handling source selection information and proprietary proposals. It is the policy of DHS S&T to treat all proposals as sensitive competitive information, and to disclose their contents only for the purpose of evaluation.

Awards may take the form of contracts or other transactions agreements (OTAs). In the event an offeror or subcontractor is a Federally Funded Research and Development Center (FFRDC), Department of Energy National Laboratory, or other Federally funded entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 U.S.C. 1531) or other appropriate authority.

Depending on the nature of the full proposals received, DHS S&T will also consider awarding a grant or cooperative agreement. Therefore, the applicable laws and regulations governing the legal vehicle used for award will depend on the legal vehicle chosen by DHS S&T. In this regard, offerors should propose a preferred vehicle type for DHS S&T to consider for award.

I. GENERAL INFORMATION

1. Agency Name

Department of Homeland Security

Science & Technology Directorate

Washington, DC 20528

2. Research Opportunity Title

Ubiquitous Biological and Chemical Sensing

3. Program Name

CELL-ALL

4. Research Opportunity Number: BAA07-10

5. Important Dates

Event Date Time (local Eastern Time)

White Paper Due Date **11/29/2007** 4:30 P.M.

Notification of Evaluation of White Papers 12/14/2007 N/A

Full Proposal Due Date **01/14/2008** 4:30 P.M.

(A Full Proposal will not be accepted unless a White Paper was received before the White Paper due date specified herein AND the Offeror was encouraged to submit a Full Proposal.)

Notification of Evaluation of Full Proposals/Recommendation for Award 02/08/2008 N/A

* There is a registration process (see Section 4 of this BAA). A Prospective Offeror must ensure that it allow itself sufficient time to complete the registration and submission process. Extensions will NDT be granted.

Oral Presentations – Prospective Offerors are NOT provided the opportunity to make oral presentations.

6. Research Opportunity Description -

DHS S&T has designated this program as a High Impact Technology Solution (HITS), which is designed to a provide proof-of-concept answers within one to three years that could result in high-payoff technology (revolutionary) breakthrough. DHS S&T is seeking out those innovative, "out-of-box', possibly disruptive technologies (disrupting the normal evolutionary technological development process). It is recognized that this project will have considerable technological risk; however it also offers the potential for significant gains in capability.

Innovation is critical. Offerors should demonstrate that their efforts are aimed at high-risk/high-payoff technologies that have the potential for making revolutionary rather than incremental improvements to homeland security, including emerging threats and operational challenges. ***DHS S&T reserves the right to select for award and fund all, some, or none of the Full Proposals received in response to this solicitation.***

Today's biological and chemical sensing networks work effectively to cover limited and specific physical areas and environments with significant cost and overhead. In order to greatly expand coverage and realize greater WMD protection for the nation, a revolutionary breakthrough that provides for a much larger and lower cost sensing distributed network is required. For example, if biological and chemical sensors could be effectively integrated into common cell phone devices and made available to the American public on a voluntary basis, the Nation could potentially benefit from a sensor network with more than 240M sensors. Through this BAA, HSARPA is seeking to accelerate advances in miniaturized biological and chemical sensing (e.g. laboratories on a chip) with integration into common device(s) and a communication systems concept for large scale multi-sensor networks. This proof of concept should be capable of detecting hazardous biological and/or chemical materials with eventual expansion to the detection of explosive and eventually radiological materials (in future collaborations with other organizations). In the first year, proposed work should lead to a minimum of a relevant laboratory demonstration of a proof-of-concept sensor, device and communications system for Cell-All. Optional second year work may be proposed to build upon success in year one and may include additional field experiments and characterizations.

The proposed concept should develop a miniaturized sensor, device and system that when integrated is capable of addressing the following performance characteristics:

• Integrated into a common domestic platform, such as a cell phone

• User enabled so that the device can be switched on or off at the discretion of an individual user.

• Low cost and easy to maintain at scale

• Capable of accurately and securely communicating the location, date, time and binary outcome of sample readings

• Capable of receiving and displaying warning information from operations centers

• Demonstrates significant potential to provide accurate readings in a wide variety of environments

• Provides adequate sample collection methods within the host device to enable accurate sensing

• Provides sensing capability for multiple samples and any required methodology to readily refresh consumables

• Provides a reasonable power profile that does not significantly degrade the performance of the host device

• Survives a variety of environmental conditions

• Demonstrates an effective lifetime of more than one year.

• Supported by developmental architectures and development environments that promote low cost experiments, spiral prototyping and wide scale implementation

The contractor will also:

• Clearly define risks and vulnerabilities of the recommended technical approach and address methods to mitigate those risks and vulnerabilities

• Identify any barriers to ubiquitous sensing using the collection and sensor devices as proposed

• Provide a rough order of magnitude estimate of costs and overall schedule to develop each component and integrate into an overall system.

• List relevant experience in efforts that are similar

DHS S&T is receptive to individual or team offers. Technology developers must describe the schedule of incremental products they expect to produce.

7. Government Representatives

Science and Technology
Stephen Dennis, Program Manager
Department of Homeland Security
Science and Technology (S&T) Directorate
Washington DC, 20528

Business
Margaret L. "Margo" Graves
Team Lead/Contracting Officer
Department of Homeland Security
Office of Procurement Operations/

"Proposal White Paper"

BROAD AGENCY ANNOUNCEMENT (BAA) 07-10

CELL-ALL Ubiquitous Biological and Chemical Sensing

Administrative and Technical Points of Contact:

Larry Golden, CEO
ATPG Technology, LLC
522 Peach Grove Place
Mauldin, SC 29662
864-288-5605 / 864-992-7104
Lgolden5605@charter.net

Executive Summary:

Two years ago, recognizing the danger that existed if a WMD was concealed, transported and deployed within our borders, ATPG embarked on the development of a multi-sensor, tracking and detection system. The first development spiral yielded a functional Sensor Monitoring Device (SMD) prototype and tiered communication applications to distribute, monitor and manage the multi-sensor SMD network information. The ubiquitous sensor network solution proposed in this white paper borrows heavily from the technology developed in spiral one. The tiered communication, viewer and management software applications were designed to be part of a large sensor network. For this application the software will be scaled and enhanced to accommodate the volume of traffic that would result from an extremely large sensor network.

Our SMD was designed to provide as much flexibility as possible and communicates with a variety of sensors through an array of built-in standard interfaces (SPI, A/D, Serial, Bluetooth, I2C etc). This existing open architecture design affords us the opportunity to collaborate with the U.S. Army Edgewood Chemical and Biological Center (ECBC) to evaluate, test and acquire the most appropriate miniaturized chemical and biological sensors.

ATPG intends to utilize the hardware and software technology developed in spiral one as the basis for the ubiquitous sensor network. The form factor of the SMD will be re-engineered so that it can initially be housed in cell phone cases allowing straightforward integration with existing cell phones. The SMD, housed in the cell phone cases will use a Bluetooth channel to communicate with ATPG software hosted on the cell phone. This software will provide bidirectional communication between the SMD and cell phone. The cell phone software will additionally use email and SMS messaging services to communicate information to control centers. The software for managing the information from the sensor network will be architected in a way that provides a means to efficiently escalate information up the government hierarchy.

The software will employ a large database back-end and where practical message routing rules will be implemented to allow for effective and efficient routing of sensor message traffic.

Utility to Department of Homeland Security:

ATPG's strategy of incorporating its existing SMD design into cell phone cases provides a means to quickly establish a massive sensor network nationwide. ATPG proposes modifying the SMD form factor so that it can be installed into the most common cell phone cases. When a person volunteers for the program they would receive a cell phone case along with an adapter

cord that would connect to their existing phone charger; allowing the SMD and phone to charge simultaneously. A switch on the case will allow the volunteer to enable the device at their discretion. If a volunteer elects to participate in the program and their cell phone does not have an on board GPS, the SMD provided in the cell phone case will be equipped with one. The geographic position of the SMD/cell phone pair will be determined either by GPS, cell phone tower database and signal strength or by a Wi-Fi hotspot database. In the event current position cannot be determined, the device will use its last known good position fix for communications and the position will be flagged as such. Housing the SMD and sensors in a cell phone case provides a number of advantages. Since the SMD will draw all of its power from its own power source the only resources required from the cell phone will be for a dedicated Bluetooth channel and limited processing power to execute the cell phone software. Additionally the consumables in the cell phone case (battery, sensors etc.) can easily be switched out, or the entire case can be easily replaced. ATPG will be working with the Otter Box Company to design a cell phone case capable of housing the SMD and its sensors, providing a protective, water resistant case while maintaining complete cell phone interactivity. This approach will allow ATPG to easily and incrementally make changes to the host platform as the technology of the SMD and its sensors are miniaturized.

Technical Approach:

The creation, implementation and management of a massive sensor network will require a design approach that delivers a system solution. Every tier of the system is important and the end product must be manageable, provide redundancy and implement an open architecture wherever possible. The ATPG solution proposed here focuses on these requirements and delivers a design that translates into a straightforward, deployable sensor network system that can be distributed en masse.

At the lowest level, the SMD is engineered to communicate with a variety of sensors through an array of standard interfaces (SPI, A/D, Serial, I2C etc). This open architecture allows for easily integrating additional sensors into the device and expanding the range of hazardous agents detectable by the SMD. The SMD will continually monitor/control the attached sensors and communicate with the cell phone via a dedicated Bluetooth channel. When the SMD is activated by the user, a small software application installed on the phone will monitors the

Bluetooth channel for detection alerts and also forward commands received from control centers to the SMD. The SMD will periodically send its position information to the control center. The position the SMD will report to the control centers is determined using a layered approach.

Initially the SMD will look to the on-board GPS (if provided) to determine position. If the cell phone is equipped with a GPS the application on the cell phone will retrieve the position from its own GPS. When a GPS position cannot be determined, the position of the SMD and its user will be calculated based on a cell phone tower database, provided by the FCC and signal strength. If this does not yield a result, the Wi-Fi hotspot database will be utilized to determine SMD and user position. If all these options fail, the last known position can be augmented with the on board accelerometers to estimate the current position which will be reported to the control centers and annotated as a last position and a possible position. All information received by the cell phone application from the SMD will be forwarded to the control centers either through email or SMS messages if email is not available. The information transmitted will be encoded in XML and encrypted prior to transmission. When a user needs to be notified of information from a control center, the cell phone software will use either a ring tone or vibration to call the user's attention to the display. This solution of integrating the SMD into the cell phone case and installing a small software application on the volunteer's cell phone provides a means to easily modify and upgrade the sensor network system as advancements are made to sensor and SMD technology with minimal impact to the user.

The web and desktop software that support the sensor network is designed to support an escalating reporting hierarchy. At each level rules can be established in the message routing software to facilitate the transfer of alert information. Rules can also be established to assist in determining the area affected by an alert. In the event a chemical or biological agent is detected and reported, the software can automatically search for other sensors in a pre-defined area and command them to sample and report back. This information can then be used by first responders and local government to determine the impacted area and aid in creating a plan of action to cope with the event. The reporting hierarchy can be configured as needed but the current configuration sends notification to the local First Responder units, followed by City, County, State and Federal government. As the information works its way up the hierarchy rules at each level fire off to create events that notify necessary personnel at each level. The viewer/management software used at each level of the hierarchy is identical. How the system forwards and responds to data is

configured in the message routing rules table. The desktop software uses Google Earth as a viewer and plots the position of the sensors and detections on the map. Filtering options are provided in the software to allow the screen to be decluttered. A hierarchical database of sensors reporting to the viewers at a given control center is maintained to allow simple manipulation of the sensor network. The software will allow the user to drill down into lower levels of the data by clicking on the images on the map or through the windows explorer like interface provided.

The software will also allow commands and alerts to be sent to SMD enabled cell phones by clicking on the image or on its text representation. Each SMD representation on the map will display its unique identification number as its label and clicking on the icon will display the last set of data received by the control center. The sensor network data can also be made available to smart phones and PDAs running a variation of the viewer/management software. All data passed through this network will be encrypted and all database and user accounts will be protected by multiple layers of security to ensure the privacy of the volunteers and protect their location from foreign/unwanted access.

As an option all messages sent from the SMD to the control centers could receive notification of receipt; confirmation that the network is operating properly. This could be a built-in fail safe, which would allow the user to be notified first if detection occurred and the information could not be transmitted to a control center. In this scenario the user would be notified of the detection and could take action to leave the area and contact authorities through some other means.

Personnel and Performer Qualifications and Experience:

Larry Golden is the CEO of ATPG and will be the project manager for this program. Mr. Golden's invention and patent pending sensor monitoring device (Pub. 10-18-07; App. #: 11/397,118) will be used as the departure point for the development of the SMD. Mr. Golden's background is in industrial engineering and management. Larry's duties will include managing the schedule, budget and subcontractors providing the cell phone cases.

Harold Kimball is a software engineer with twenty years' experience developing software applications, including embedded systems, operational flight programs, database applications, and web and desktop applications. Mr. Kimball will be the technical lead on this program as well as the lead software developer for the SMD applications. Over the past few years Mr. Kimball's focus has been on developing situational awareness applications, embedded device applications

and aircraft simulation software. Mr. Kimball has a Bachelor's degree in Computer Science and is working on his Master's Degree in Artificial Life. Mr. Kimball recently had an article published describing a scalable disaster relief and communications infrastructure system he is developing to aid first responders and disaster relief personnel in their efforts.

Doug Cumbie is an electrical engineer and software engineer with six years' experience developing embedded systems, web applications, situational awareness software and aircraft simulation software. Mr. Cumbie will be the lead Engineer on this program as well as the primary developer for the web and desktop applications. Over the past few years Mr. Cumbie has focused on embedded device development, situational awareness applications and aircraft simulation software. Mr. Cumbie holds Bachelor's degrees in both Computer Engineering and Electrical Engineering.

The Otter Box Corporation will provide custom cell phone cases for housing the SMD developed by ATPG. The Otter Box Corporation has extensive experience manufacturing and distributing custom cases for cell phones, laptops and PDAs. Their manufacture and distribution experience will play a key role in the ability to efficiently develop, manufacture and distribute a custom cell phone case enveloping the SMD and providing a water resistant and protective case. U.S. Army Edgewood Chemical and Biological Center (ECBC) will play a vital role in assisting ATPG with evaluating, testing and selecting the most appropriate miniaturized chemical and biological sensors available. ATPG and ECBC have a collaborative agreement in place ensuring ATPG of their services in sensor analysis and selection.

Commercialization and Capabilities:

ATPG will work closely with Otter Box and ECBC to determine the physical characteristics and requirements needed to create a custom cell phone enclosure for the selected sensors and SMD. ATPG will leverage Otter Box's manufacturing and distribution experience to enable ATPG to produce and deliver large quantities of custom cell phone cases. As mentioned previously the case will be designed and developed so that consumables can easily be swapped out or the entire cell phone case can be replaced. This approach ATPG is pursuing is the most economical and efficient way to mass distribute a sensor network; providing low risk and minimal impact to volunteers of the program. Becoming part of this volunteer network would be a simple process and would only require end-users to; elect to become a volunteer, indicate which type of cell phone they currently use and upon receipt of the new cell phone case

commence holstering the cell phone in the case wherever they go. As an option and to solicit interest in the program, volunteers could be provided software applications. These applications could potentially access tracking information of the volunteer's phone and the volunteer's family members' phones; or a moving map application could be provided to enable navigation through the cell phone. Mr. Kimball and Mr. Cumbie have many years' experience developing and distributing code to demanding end users. Both individuals have experience providing Situational Awareness and OFP software to the Air Force Special Operations Command (AFSOC) for all fixed wing Special Operations Forces (SOF) aircraft. Additionally, Mr. Kimball worked for Manheim Auctions, an international organization with a large customer base and participated in the development and distribution of Manheim's software applications.

One method ATPG conceived for fielding the sensor network and implementing its widespread use would be to conduct a pilot program for the nearly 30 million government employees, border patrol personnel and government contractors. These individuals generally work in what would be considered high value target areas. Providing these employees with cell phone cases equipped with the SMD and its sensors would immediately give the sensor network nationwide coverage in many areas that would be likely targets of a terrorist attack. In addition to gaining nationwide coverage; if this pilot program extended to all government employees and its contractors around the world, the network would have the ability to monitor U.S. interests globally.

Costs, Works and Schedule:

The budgeted cost for this development is $1,000,000, with a projected period of performance of one year. ATPG will simultaneously commence four primary tasks upon contract award.

1) ATPG will work with ECBC to evaluate, test and select the most appropriate chemical and biological miniaturized sensors available (4 month effort, $17,137)).

2) ATPG will research and determine the three most commonly used phones capable of being part of this sensor network and work with Otter Box to design and manufacture cell phone cases to house the SMD and sensors (4 month effort, $45,000).

3) ATPG will enhance/scale the software applications to support the potentially large volume sensor network that will comprise the Cell-All ubiquitous system (7 month effort, $500,000).

4) ATPG will restructure and scale down the SMD so it can be accommodated in the cell phone case. After month 7, integration and testing of the Cell-All system will commence. The system will be documented (block diagrams, wiring diagrams, and theory of operation manual) and a demonstration date will be scheduled (12 month effort, $437,863).

Prototype cases housing the SMD and sensors, cell phones and viewer/management software executables will be delivered upon project completion.

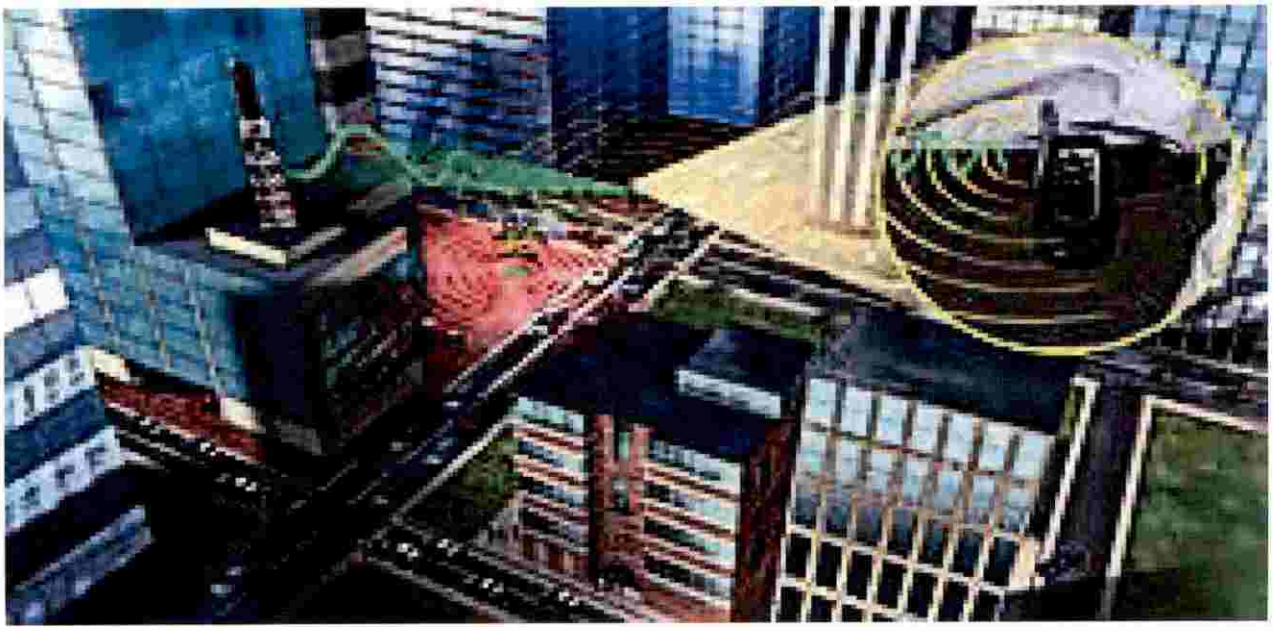
Small Business Considerations:

This white paper is submitted from a minority owned small business.

Official website of the Department of Homeland Security

2010 Archives

Cell-All: Super Smartphones Sniff out Suspicious Substances



Years ago, if you wanted to take a picture, you needed a dedicated camera. You needed to buy batteries for it, keep it charged, learn its controls, and lug it around. Today, chances are your cell phone is called a "smartphone" and came with a three-to-five megapixel lens built-in—not to mention an MP3 player, GPS, or even a bar code scanner.

This Swiss Army knife trend represents the natural progression of technology—as chips become smaller and more advanced, cell phones continue to absorb new functions. Yet, in the future, these new functions may not only make our lives easier, they could also protect us—and maybe even save our lives.

The Cell-All initiative may be one such savior. Spearheaded by the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), Cell-All aims to equip your cell phone with a sensor capable of detecting deadly chemicals at minimal cost—to the manufacturer (a buck a sensor) and to your phone's battery life. "Our goal is to create a lightweight, cost-effective, power-efficient solution," says Stephen Dennis, Cell-All's program manager.

How would this wizardry work? Just as antivirus software bides its time in the background and springs to life when it spies suspicious activity, so Cell-All regularly sniffs the surrounding air for certain volatile chemical compounds.

When a threat is sensed, a virtual *ah-choo!* ensues in one of two ways. For personal safety issues such as a chlorine gas leak, a warning is sounded; the user can choose a vibration, noise, text message, or phone call. For catastrophes such as a sarin gas attack, details—including time, location, and the compound—are phoned home to an emergency operations center.

While the first warning is beamed to individuals—a grandmother taking a siesta or a teenager hiking through the woods—the second warning works best with crowds. And that's where the genius of Cell-All lies—in crowdsourcing human safety.

Currently, if a person suspects that something is amiss, he *might* dial 9-1-1, though behavioral science tells us that it's easier to do nothing. If he does do something, it may be at a risk to his own life. And as is often the case when someone phones in an emergency, the caller may be frantic and difficult to understand, diminishing the quality of information that's relayed to first responders. An even worse scenario: the person may not even be aware of the danger, like the South Carolina woman who last year drove into a colorless, odorless, and poisonous ammonia cloud.

In contrast, anywhere a chemical threat breaks out—a mall, a bus, subway, or office—Cell-All will alert the authorities automatically. Detection, identification, and notification all take place in less than 60 seconds. Because the data are delivered digitally, Cell-All reduces the chance of human error. And by activating alerts from many people at once, Cell-All cleverly avoids the longstanding problem of false positives. The end result: emergency responders can get to the scene sooner and cover a larger area—essentially anywhere people are—casting a wider net than stationary sensors can.

But what about your privacy? Does this always-on surveillance mean that the government can track your precise whereabouts whenever it wants? To the contrary, Cell-All will operate only on an opt-in basis and will transmit data anonymously. "Privacy is as important as technology," avers Dennis. "After all, for Cell-All to succeed, people must be comfortable enough to turn it on in the first place."

For years, the idea of a handheld weapons of mass destruction detector has engaged engineers. In 2007, S&T called upon the private sector to develop concepts of operations. Today, thanks to increasingly successful prototype demonstrations, the Directorate is actively funding the next step in R&D—a proof of principle—to see if the concept is workable.

To this end, three teams from Qualcomm, the National Aeronautics and Space Administration (NASA), and Rhevision Technology are perfecting their specific area of expertise. Qualcomm engineers specialize in miniaturization and know how to shepherd a product to market. Scientists from the Center for Nanotechnology at NASA's Ames Research Center have experience with chemical sensing on low-powered platforms, such as the International Space Station. And technologists from Rhevision have developed an artificial nose—a piece of porous silicon that changes colors in the presence of certain molecules, which can be read spectrographically.

Patent Claim A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:

a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological

sensor;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.

Continue from DHS official site: Similarly, S&T is pursuing what's known as cooperative research and development agreements with four cell phone manufacturers: **Qualcomm, LG, Apple, and Samsung.** These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. As a result, Dennis hopes to have 40 prototypes in about a year, the first of which will sniff out carbon monoxide and fire.

To be sure, Cell-All's commercialization may take several years. Yet the goal seems imminently achievable: Just as Bill Gates once envisioned a computer on every desk in every

home, so Stephen Dennis envisions a chemical sensor in every cell phone in every pocket, purse, or belt holster. If it's not already the case, our smartphones may soon be smarter than we are.

To request more information about this story, please e-mail st.snapshots@hq.dhs.gov.

THE GOVERNMENT ENTERED INTO AGREEMENTS WITH APPLE, SAMSUNG, LG, AND QUALCOMM FOR THE DEVELOPMENT AND COMMERCIALIZATION OF THE 'CMDC' DEVICE (i.e. Modified CELL PHONE). APPLE, SAMSUNG, LG, AND QUALCOMM's INFRINGEMENT OF THE COMMUNICATING, MONITORING, DETECTING, AND CONTROLLING (CMDC) DEVICE IS ILLUSTRATED BELOW.

"TESTING MECHANISM CLAIM CHART" TO DETERMINE INFRINGEMENT

Read from Left>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> to >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>Right>>>>>>>>>>>

Apple's iPhone 5, 5c, 5s, 6, 6, 7, 8, 9, and 10 and the iPad interconnected to the Apple Watch	**Patent #: 9,589,439; Independent Claim 22**	**Patent#: RE 43,990; Dependent Claims**
The Apple Watch (e.g. multi-sensor detection device: interconnected to monitoring equipment – iPhone / iPad; biosensor for detecting heart rate; leveraged internet and GPS connections; power source battery; CPU; light indicators). Apple Watch requires an iPhone 5, 6, 7, 8,9, and 10.	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:	18. The communication device of claim 11 wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring

The heart rate bio-chemical sensor in Apple Watch uses photoplethysmography (heart rate (HR) and pulse oximeter oxygen saturation (SpO2) from wearable photoplethysmographic (PPG) biosensors). Technology based: Apple Watch can calculate the number of times the heart beats each minute; your heart rate.	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;	118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.
Apple chip A8X delivers better CPU and graphics performance than its predecessor. With its 64-bit desktop-class architecture, iPad Air 2 is as powerful as many personal computers. It's power efficient, too, with a 10-hour battery life. The iPhone 6's A8 processor has a dual-core model like the A7, but clocked at a higher frequency. The iPhone 6 has a 2GHz dual-core 20nm 64-bitA8 CPU.	at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).
If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen	a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

If your iPhone, iPad, or iPod touch is lost or stolen. Turn on Lost Mode. Using Lost Mode, a person can remotely lock the device with a four-digit passcode, and display a custom message with your phone number on your missing device's Lock screen	a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Every iPhone and iPad ever made has both WiFi and Bluetooth. The cellular service, originally called 3G and now called LTE; allows the iPhone to connect to the internet anywhere cell phone works. The iPhone uses the GPS chip in conjunction with cell phone towers and Wi-Fi networks—in a process termed "assisted GPS".	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). iPhone and iPad Touch ID use fingerprint as a passcode. Fingerprint one of best passcodes in the world. With just a touch of the device's Home button, the Touch ID sensor quickly reads a fingerprint and automatically unlocks the phone.	the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...

If Apple Touch ID doesn't recognize your finger after multiple failed attempts, you'll be given the option of entering your Apple ID password. You need to enter your Apple ID password after: (1) Restarting your device, and (2) Enrolling or deleting fingers. If lost or stolen, you can disable Touch ID from being used to unlock your device with Find My iPhone Lost Mode. Additional protection against theft with Activation Lock,	the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;	22. The communication device [of claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop
iPhone and iPad Touch ID is a seamless way to use your fingerprint as a passcode. Your fingerprint is one of the best passcodes in the world. With just a touch of your device's Home button, the Touch ID sensor quickly reads your fingerprint and automatically unlocks your phone.	the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...
NFC arrived on the iPhone 6 in 2014, it has been restricted to the contactless Apple Pay system. But at the Worldwide Developers Conference last week, Apple quietly announced that with the arrival of iOS 11 this fall, apps will be able to use an iPhone's NFC chip to read tags, pair with accessories, and exchange data with other NFC devices.	the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.

Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails. The iPhone's GPS chip is like that found in stand-alone GPS devices. The iPhone uses the GPS chip in conjunction with cell phone towers and Wi-Fi networks—in a process termed "assisted GPS"—to quickly calculate the phone's position.	whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Every iPhone and iPad ever made has both WiFi and Bluetooth, two wireless technologies for connecting to nearby devices (in the case of Bluetooth) and the internet (in the case of WiFi). The cellular service, originally called 3G and now called LTE; this option allows the iPhone to connect to the internet anywhere cell phone works, to check emails. Apple chip A8X delivers better CPU and graphics performance than its predecessor. The iPhone 6's A8 processor has a dual-core model like the A7. The iPhone 6 has a 2GHz dual-core 20nm 64-bit A8 CPU.	wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

Samsung Galaxy s6 interconnected to the "Samsung Gear S2 Smartwatch"	**Patent #: 9,589,439; Independent Claim 22**	**Patent#: RE 43,990; Dependent Claims**
The Samsung Gear S2 smartwatch (e.g. multi-sensor detection device: interconnected to monitoring equipment – Samsung Galaxy s6; biosensor for detecti ng heart rate; leveraged internet and GPS connections; power source battery) has a solid health tracking and slightly better battery life than other high-end smartwatches. It works with a variety of Android phones.	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:	18. The communication device of claim 11 wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring
The Gear S2 need to connect to a mobile device (e.g. Galaxy S6) using the Samsung Gear application. The application must be installed on the mobile device (e.g. Galaxy S6). The Gear S2 sensors include: Accelerometer; Gyroscope; Heart Rate; Ambient Light;, and, Barometer. Connectivity include: 802.11n WiFi; Bluetooth 4.1; NFC. GPS include: The Gear S2 3G includes a GPS receiver and two apps, Nike+ and S Health, that include GPS tracking support.	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;	118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the eell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.

Samsung Galaxy s6 CPU (Central Processing Unit) - otherwise known as a processor - is an electronic circuit that can execute computer programs. The Samsung Galaxy S6 SM-G920i 32GB is a good Android phone with 2100 MHz processor 8-core that allows the user run heavy applications. The Samsung Galaxy S6 smartphones and tables don't just use "processors", they use what's called a System-on-a-chip (SoC). The SoC is the equivalent of a computer motherboard, including main processor, graphics processor and memory, on a single chip. The CPU is nonetheless a must-have component of the SoC. Modern SoCs have two, and soon four, processors cores ("multi-core")	at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).
The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Samsung Galaxy S6 "Fingertip Heart Rate Monitor" detection device (e.g. cell phone detection device) is a built-in monitor that measures heart rate from a fingertip using a biosensor.	a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

The Samsung Galaxy S6 capable of receiving a signal to reset (e.g. unlock; locking device) the phone. The Samsung Galaxy S6 "Fingertip Heart Rate Monitor" detection device (e.g. cell phone detection device) is a built-in monitor that measures heart rate from a fingertip using a biosensor.	a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Cellular data connection: The connection that the Galaxy s6 uses to exchange data over the air using your mobile operator's cellular network. Cellular network connection: the Galaxy s6 uses for voice and data connect. This network is managed by the mobile operator. WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot. Bluetooth: v4.1, A2DP,LE,	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
Seven wireless interfaces in the Samsung Galaxy S6 smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging. Samsung allows 4 fingerprints to set-up the fingerprint scanner; for log-in and lock-out. Samsung's Face unlock uses the front-facing camera to identify the user and unlock the device. Samsung's iris scanning method, uses special sensors on front of phone to identify and unlock the device.	the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.

After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up as a security feature. If user is unable to log in after doing all the security layers, there's no other option but to have the phone unlocked. Samsung's near-field communication (NFC) enabled smartphone: slide hand on the back and the NFC Ring can unlock it. The NFC Ring comes with two special NFC tag inlays inside the ring. The NFC Ring can be used to unlock & control mobile devices	the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;	22. The communication device [of claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop
Samsung only allows you to register 4 fingerprints to set-up the fingerprint scanner; a security feature for easy log-in and lock-out. Samsung's new Face unlock feature uses the front-facing camera to identify the user and unlock the device. Samsung has included an iris scanning method, which uses special sensors on the front of the phone to identify you and unlock the device. Iris scanning is considered one of the most secure biometric methods	the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.
Seven wireless interfaces now found in the Samsung Galaxy S6 high-end smartphone - Frequency Division Duplex Cellular, Time Division Duplex Cellular, Wi-Fi, Bluetooth, GNSS (Global Navigation Satellite System), Near-Field Communication, and Wireless Charging	the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.

Cellular data connection: The connection that the Galaxy s6 uses to exchange data over the air using your mobile operator's cellular network. Cellular network connection: The network that the Galaxy s6 uses for making voice and data connections. This network is managed by the mobile operator.WLAN: Wi-Fi 802.11, Wi-Fi Direct, and hotspot. Bluetooth: v4.1, A2DP, LE, apt-X. The Galaxy can determine location using its built-in Global Positioning System (GPS) transmitter, Wi-Fi networks, and mobile networks.	whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.
The Samsung Galaxy S6 capable of automatically transmitting a signal to lock after several failed log-in attempts. The Samsung Galaxy S6 capable of receiving a signal to reset (e.g. unlock; locking device). Thereby activating or deactivating a security system.	wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

LG Electronics: LG V10 Smartphone; LG Watch Sport	**Patent #: 9,589,439; Independent Claim 22**	**Patent#: RE 43,990; Dependent Claims**
2008: The "Cell-All" initiative. The DHS-S&T, Cell-All aims "to equip your cell phone with a sensor capable of detecting deadly chemicals", says Stephen Dennis, Cell-All's program manager. S&T pursued cooperative agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. Used by the Government; 2016: Both the LG G5 and V10 smartphones is used by the Department of Defense. Sensors will integrate with 261 million cell phones.	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:	18. The communication device of claim 11 wherein the communication device having a basic monitoring terminal can be adapted and incorporated to include desktop computers, notebook, PC's, laptops, cell phones, smart phones, LCD monitors, and satellite monitoring
The LG Watch Sport is, well, sporty-looking with a big 1.38-inch, 480-by-480 P-OLED display. The device has two buttons for convenient navigation and integrates multiple sensors, including an accelerometer, barometer, ambient light, GPS, and a PPM sensor (short for photoplethysmogram, which accurately tracks heart rate when the wearer is at rest or active).	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;	118. The multi-sensor detection system [of claim 103] wherein the cell phone, the smart phone, and the cell phone detector case have a plurality of sensors for detecting at least one of a chemical, biological, radiological, nuclear, explosive and contraband agents and compounds which are capable of being disposed within the cell phone, the smart phone, or the cell phone detector case.
LG V10 CPU: Hexa-core (4x1.4 GHz Cortex-A53 & 2x1.8 GHz Cortex-A57). LG smartphones are equipped with embedded chipsets. The CPU that's at the core of the chipset is vital for general computing performance. LG V10 Chipset: Qualcomm MSM8992 Snapdragon 808	at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;	12. The communication device [of claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).

Transmits signals through at least one of a cellular, a long or short range radio frequency, or a Bluetooth connection. You can use Bluetooth to transfer information between LG V10 phone and another Bluetooth-enabled device. Quick message is the specified text message to send out.	a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
Receives signals through at least one of a cellular, a long or short range radio frequency, or a Bluetooth connection. LG V10 User Guide: Notifications: Enable this option if you wish to receive a notification when a new text or multimedia message arrives.	a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.
LG V10 cellular connection; Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, DLNA, hotspot; Bluetooth 4.1, A2DP, LE, aptX; GPS with A-GPS, and GLONASS	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.

LG V10 features include sensors for face/smile detection, iris scanner, and fingerprint recognition.	the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...
After 5 unsuccessful attempts to unlock the LG smartphone, the user is prompted to enter a text phrase to confirm that they are trying to unlock the phone. After 10 unsuccessful attempts, the phone will automatically perform a factory data reset and all of the personal files will be erased.	the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;	22. The communication device [of claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop
LG V10 features include sensors for face/smile detection, iris scanner, and fingerprint identification.	the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;	30. The communication device [of claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature...

The LG V10 NFC is a short-range high frequency wireless communication technology that enables the exchange of data between devices over about a 10 cm distance. It allows users to share content between digital devices, and even use their LG smartphone on existing contactless infrastructure. The significant advantage of NFC over Bluetooth is the shorter set-up time (under a 1/10 second).	the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;	20. The communication device [of claim 11] wherein the communication device can be interconnected through wire or wireless for communication, signals, commands and transmission of data.
LG V10 cellular connection; Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, DLNA, hotspot; Bluetooth 4.1, A2DP, LE, aptX; GPS with A-GPS, and GLONASS. Smartphone manufacturers and operators have introduced the Assisted GPS technology, which downloads the current ephemeris for a few days ahead via the wireless networks and helps triangulate the general user's position with the cell towers thus allowing the GPS receiver to get a faster lock at the expense of several (kilo) bytes.	whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and	25. The communication device [of claim 11] wherein the communication device has at least one of a Bluetooth connection, a Wi-Fi connection, a short and long range radio frequency connection, a Cellular connection, a satellite connection, and a GPS connection.

Transmits and receives signals through at least one of a cellular, a long or short range radio frequency, or a Bluetooth connection. You can use Bluetooth to transfer information between LG V10 phone and another Bluetooth-enabled device. Quick message is the specified text message to send out. LG V10 User Guide: Notifications: Enable this option if you wish to receive a notification when a new text or multimedia message arrives.	wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).	28. The communication device [of claim 11] wherein the communication device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to and from a cell phone, smart phone, PDA or handheld device.

ITC Provides Clarity on the Meaning of a Section 337(a)(2) "Article"

ITC Provides Clarity on the Meaning of a Section 337(a)(2) "Article"

A recent decision by the International Trade Commission ("ITC" or the "Commission") held that pre-commercial or non-commercial items qualify as "articles" for purposes of section 337 investigations.[1]The decision opens up the ITC to complainants who are in an earlier phase of product development. Under section 337(a)(2), a Complainant bears the burden to show that the "domestic industry requirement" is satisfied by showing that an industry in "*articles* protected by the patent, copyright, trademark, mask work, or design concerned, exists or is in the process of being established."[2] The question that remained was whether the protected article had to be in production. In its 1046 Investigation opinion, the Commission has provided some much-needed clarity.[3] In reversing the Initial Determination, the Commission held that Section 337(a)(2) "does not require commercial production for a domestic industry in the process of being established."[4]

In the 1046 Investigation, Complainant Macronix asserted that a domestic industry in the process of being established existed based on its research and development on an experimental semiconductor wafer as its "article."[5] While the Macronix product was not a commercial product at the time of filing the complaint, or the hearing, Macronix argued that the domestic industry requirement does not require showing that the domestic industry article is a mass-produced or commercialized product.[6] The Macronix product was not ready for the marketplace, but a small quantity of precursors were made for the purpose of further research and development, and, Macronix argued, the product practices the asserted patents.[7]

In the Initial Determination, ALJ Lord agreed with Respondent Toshiba, and held that while Section 337 allows for complainants seeking to protect "nascent industries" to prevail by showing a domestic industry "in the process of being established,' the statute nevertheless requires a showing of an "article of commerce, *i.e.*, a product for sale in the marketplace" to satisfy the "article" requirement of the Section 337(a)(2) domestic industry requirement.[8] Thus, ALJ Lord held that within the provisions and purpose of Section 337(a)(2), "article" refers to "products or other commodities that are sold in the marketplace."[9] According to the ID, Macronix's product was not "commercially viable" and, therefore, Macronix did not satisfy the domestic industry requirement, and no exclusion order should issue.

After both sides and the OUII Commission Staff appealed to the Commission, the Commission reversed the ID and issued a limited exclusion order against Respondent Toshiba.[10] The Commission disagreed with the ALJ's interpretation of "article" under section 337(a)(2), and stated that commercialization is *not* a prerequisite for proving a domestic industry based on an industry in the process of being established, and that a domestic industry may be based on a product still in the pre-commercial or non-commercial stage.[11]

The Commission explained that the term "article" is "sufficiently capacious to embrace pre-commercial or non-commercial items."[12] The holding cites a previous Commission opinion which cautioned against an interpretation of "article" that "would offer no relief to an inventor-complainant ... before the complainant has had an opportunity to engage in production-oriented efforts."[13] The Commission also relied on the legislative history of Section 337 to support its holding that an "article.' need not be commercialized. Using Section 337(a)(3)(C) as an example that permits a domestic industry based on licensing activities, the Commission stated

that Congress clearly intended to provide a remedy to nascent industries such as universities, inventors, and start-ups in the absence of a commercialized product where those industries would use licensing to raise the funds needed to manufacture a product.[14]

While the two-part test[15] for proving a domestic industry *in the process of being established* remains a difficult evidentiary threshold, this Commission opinion affords complainants security in initiating an investigation to thwart a "speedy infringer" where a complainant does not yet have a commercially ready product. In other words, it is now possible for complainants to go to the ITC earlier in their development cycle. Under this Commission opinion, the ITC is now an even more favorable venue for complainants in industries with lengthy research and development timelines, such as the medical device and pharmaceutical industries; or industries with rapid product updates, such as consumer electronics.

Endnotes

---

[1] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, Comm'n Op. at 41 (Oct. 26, 2018).

[2] 19 U.S. Code§ 1337(a)(2).

[3] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, Comm'n Op. at 39-44 (Oct. 26, 2018).

[4] *Id.* at 41.

[5] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, ID at 142-44 (Apr. 27, 2018).

[6] *Id.*

[7] *Id.* at 150-54.

[8] *Id.* at 144-50.

[9] *Id.*

[10] *Certain Non-Volatile Memory Devices and Products Containing Same*, Inv. No. 337-TA-1046, Comm'n Op. at 71 (Oct. 26, 2018).

[11] *Id.* at 41.

[12] *Id.*

[13] *Id.* at 41-42 (citing *Certain Computers and Computer Peripheral Devices, and Components Thereof and Products Containing Same*, Inv. No. 337-TA-841, Comm'n Op. at 37 (Jan. 9, 2014) (rejecting the notion that the "article protected by the patent" "must be a product that came to market, or is expected to come to market, under the protective umbrella of the asserted patent that the product commercializes.")

[14] *Id.* at 42-43 (citing 133 Cong.Rec. S. 1794 (Feb. 4, 1987)).

[15] The two-part test for proving a domestic industry in the process of being established requires showing (1) "the necessary tangible steps to establish an industry in the United States" and (2) whether there is a "significant likelihood that the industry requirement will be satisfied in the future." *See Stringed Instruments*, Inv. No. 337-TA-586, Comm'n Op. at 13).

Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
12. The communication device of [claim 11] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
16. The communication device of [claim 11] wherein the communication device can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to the central processing unit (cpu).	NFC **Wireless Networking Technology Industry**	NFC chips might also be widely used in the Internet of Things. Qualcomm recently announced that it will include NXP's near-field communication (NFC) solution in the Snapdragon processor platform that powers mobile devices (e.g. smartphones), wearables (e.g. smartwatches), and automobiles

21. The communication device of [claim 11] wherein the communication device includes a power connection that is interconnected to the central processing unit (cpu) and power source can be battery, electrical, or solar.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
22. The communication device of [claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.	Home and Community **Wireless Networking Technology Industry**	Every time you call, navigate, download, store something or talk, you've got the power of Qualcomm technology to thank. Also the advancements for your car, home and community are made possible by the mobile hardware, software and standards we pioneered. Qualcomm invented many of the technologies that the world's leading networks and devices run on—connecting new industries, services and experiences that are changing everything.
22. The communication device of [claim 11] wherein the communication device is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.	Disabling Lock **Locking Industry**	Qualcomm Technologies announced SafeSwitch in September of 2014. SafeSwitch is available to customers through its Qualcomm Snapdragon 810 processors. SafeSwitch technology - addresses mobile security threat with a kill switch solution is designed to allow device owners to remotely disable their devices in the event that they're lost or stolen - and then re-enable them in the event they're found. This helps to protect sensitive, personal data and to deter device theft.

30. The communication device of [claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.	Biometrics **Biometrics Industry**	Authenticating the user and the device. Beyond secure fingerprint identification, a Snapdragon 835 Mobile Platform provides a user with an extra level of safety using Camera Security—a camera-based biometric solution for iris and facial recognition engineered to help enhance mobile device security
Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
30. The communication device of [claim 11] wherein the communication device is designed to be used with or without biometrics for authentication and identification, with at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse or signature, thereby allowing access to the product by authorized, trained, and equipped individuals and preventing access to the product by unauthorized, untrained, and unequipped individuals.	Biometrics **Biometrics Industry**	Mobile transactions are safest when they are protected by a combination of user and device authentication methods. This helps data remain secure from the moment a user logs into their device. A Snapdragon 835 Mobile Platform contains the Qualcomm Haven™ security platform—a combination of hardware, software and biometrics technologies that help to make online banking and payments more secure than ever.
39. The lock disabler system of [claim 33] wherein the automatic/mechanical lock disabler detection device has a power connection which is interconnected to the central processing unit (cpu) and includes a power source of battery, electrical or solar.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video

41. The lock disabler system of [claim 33] wherein the automatic/mechanical lock disabler detection device includes at least one of; a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are capable of being interconnected to a central processing unit (cpu) of the communication device.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon CPU uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
Complainant RE43,990 Patent Dependent Claims	**Qualcomm's Technological Capability and Industry**	**Qualcomm's Technological Capability (Description)**
55. The multi-sensor detection system of [claim 33] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and software hardware to support a smartphone's GPS, camera, gesture recognition, video
78. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.	Cellular and Wireless Modem: Smartwatches **Electronic Device Industry**	Qualcomm supplied LTE modem in the Apple Watch Series 3. TechInsights found the Qualcomm MDM9635M, a Snapdragon X7 LTE modem in the 42mm sport band model A1861 with GPS + cellular. The modem was mated with a Samsung K4P1G324EH DRAM in the watch. TechInsights said the watch contains a Qualcomm PMD9645 PMIC and a WTR3925 RF transceiver. Apple and Qualcomm are embroiled in patent infringement disputes including investigations at the U.S. ITC, around baseband modems. Apple continues to use the Qualcomm parts in watches. Apple discontinue paying Qualcomm royalties while court's in progress.

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
78. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.	Cellular and Wireless Modem: Smartphone **Mobile Device Industry**	The iPhone X A1865 uses the Qualcomm MDM9655 Snapdragon X16 LTE modem. iPhone 8; Qualcomm Modem Model A1663; plus 802.11ac Wi Fi with MIMO; Bluetooth 5.0 wireless technology; NFC with reader mode. iPhone 8 Plus; Qualcomm Modem Model A1664; plus 802.11ac Wi Fi with MIMO; Bluetooth 5.0 wireless technology; NFC with reader mode. iPhone 7; Qualcomm Modem Model A1660; plus 802.11ac Wi Fi with MIMO; Bluetooth 4.2 wireless technology; NFC with reader mode. iPhone 7 Plus; Qualcomm Modem Model A1661; plus 802.11ac Wi Fi with MIMO; Bluetooth 4.2 wireless technology; NFC with reader mode. The Qualcomm MDM9625M is a modem LTE chipset found in the Apple MG9M2CL/A iPhone 6 Plus and iPhone 6.
78. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded internet component, a global positioning (GPS) component, a navigation component, a tracking component, a cellular component, a satellite component, a short and long range radio frequency component, radio frequency (RF) sensor, radio frequency (RF) transceiver, Wi-Fi, antenna, Bluetooth, or interface/gateway component.	Wi-Fi **Wireless Networking Technology Industry**	With all the devices connecting to all the things, we knew we had to help ease overload. So we were the first to announce end-to-end commercial support for the next-generation of Wi-Fi. What does that mean? It translates into faster delivery and longer battery life for Wi-Fi devices—whether you're at home or on the go.

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
79. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded wireless and/or wired communication connection capable of sending signals and messages to a product; receiving signals and messages from a product; interconnected to at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation, monitoring site or another product comprises a built-in, embedded wireless and/or wired communication connection.	Modems **Wireless Networking Technology Industry**	Qualcomm quote: "Some say the modem is the most important part of your smartphone. We couldn't agree more. With our wireless modem inside your smartphone, you've got years of engineering keeping you connected to your great big world. And isn't that why you bought that device in the first place?"
79. The built-in, embedded multi sensor detection system of [claim 74] wherein the product includes at least one of a built-in, embedded wireless and/or wired communication connection capable of sending signals and messages to a product; receiving signals and messages from a product; interconnected to at least one of a cell phone, a smart phone, a PDA, a handheld, a laptop, a desktop, a workstation, monitoring site or another product comprises a built-in, embedded wireless and/or wired communication connection.	LTE **Wireless Networking Technology Industry**	Everyone promises smarter/better/faster, but with LTE, we actually delivered. We invented the wireless standards and fundamental technologies that mobile operators rely on to meet the explosive demand in mobile data traffic. And that means you can catch up on the latest sports clips without waiting for the network to keep pace.
104. The multi-sensor detection system of [claim 103] wherein each cell phone detector case includes an internet connection, a GPS connection, a radio frequency (RF) connection, a recharging cradle or seat, a front side, a top, a bottom, a pair of opposed sides and a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip [SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
108. The multi-sensor detection system of [claim 103] wherein the cell phone, the smart phone, and the cell phone detector case can be adapted or incorporated with cell phone towers and satellites for use with at least one of satellite communication, a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency (RF) chips, radio frequency (RF) sensors, radio frequency (RF) transceivers, and radio frequencies for short and long range transmissions interconnected to a central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
113. The multi-sensor detection system of [claim 103] wherein the cell phone, the smart phone, and the cell phone detector case includes a power connection that is interconnected to a central processing unit (cpu), and wherein a power source can be battery, electrical, or solar.	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
126. The multi-sensor detection system of [claim 125] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Qualcomm Snapdragon Processor: Smartwatches **Industry for Processors** **Electronic Device Industry**	Samsung Gear S2 3G Watch (Qualcomm Snapdragon 400 Processor); Samsung Gear S Watch (Qualcomm Snapdragon 400 Processor); LG Watch Sport (Qualcomm Snapdragon Wear 2100 Processor); LG Watch Style (Qualcomm Snapdragon Wear 2100 Processor); LG G Watch R (Qualcomm Snapdragon 400 Processor); LG Watch Urban (Qualcomm Snapdragon 400 Processor).

Complainant RE43,990 Patent Dependent Claims	Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
126. The multi-sensor detection system of [claim 125] wherein each communication device includes at least one of an internet connection, a GPS connection, a radio frequency (RF) connection, or a central processing unit (cpu).	Qualcomm Snapdragon Processor: Smartphone **Industry for Processors** **Mobile Device Industry**	Samsung Galaxy S8 (Qualcomm Snapdragon 835 Processor); Samsung Galaxy Note 8 (Qualcomm Snapdragon 835 Processor); Samsung Galaxy S7 (Qualcomm Snapdragon 820 Processor); Samsung Galaxy S5 (Qualcomm **Snapdragon 801 Processor); Samsung** Galaxy S4 (Qualcomm Snapdragon 600 Processor); LG V30 (Qualcomm Snapdragon 835 Processor); LG G5 (Qualcomm Snapdragon 820 Processor); LG G4 (Qualcomm Snapdragon 808 Processor); LG G3 (Qualcomm Snapdragon 801 Processor); LG Pro 2 (Qualcomm Snapdragon 800 Processor).
132. The multi-sensor detection system of [claim 125] wherein the internal or external remote/electrical lock disabler includes at least one of: a Blue tooth connection, a Wi-Fi connection, a short and long range radio frequency connection, an Internet connection, a Cellular connection, a Satellite connection, all of which are interconnected to the central processing unit (cpu).	Central Processing Unit (CPU) **Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video
134. The multi-sensor detection system of [claim 125] wherein a communication device, that of a cell phone, smart phone or handheld; capable of sending signals to a vehicle's operating equipment systems of at least one of, but not limited to, an ignition for starting and stopping, a lock for unlocking and locking, a horn for sounding; capable of receiving data and diagnostic information of the vehicle's operating equipment systems.	Vehicle's Operating Systems **Automobile Industry**	Every time you navigate you've got the power of Qualcomm technology to thank. All the advancements coming to your car, home and community are made possible by the mobile hardware, software and standards we pioneered. Qualcomm invented many of the technologies that the world's leading networks and devices run on.

ONE EXAMPLE OF THE ECONOMIC STIMULUS STRATEGY IS RESTORING THE ECONOMY: APPLE – STATISTICS & FACTS

Technical innovation paired with minimalistic designs and creative advertisements, as well as the leadership of the former CEO Steve Jobs, have made Apple one of the most valuable brands in the world. The company's success translates into strong brand loyalty, as well as into an unparalleled revenue growth, from 8 billion U.S. dollars in 2004 to more than 265 billion in 2018.

The company was first founded by Steve Jobs, Steve Wozniak and Ronald Wayne in 1976 in the garage of Jobs' parents. Their first product, known as the Apple I, consisted of an assembled circuit board without many of the present-day features of a computer, such as display, keyboard or mouse. The company started to slowly grow with the development of Apple II, Apple III, Apple Lisa and the first Macintosh, launched in 1984.

After a rather uneventful period, the company resurfaced in the late 1990s with a number of strategic and technological changes: in 1997, Apple introduced the Apple Online Store, followed by the iMac and the video editing program Final Cut Pro in 1998. The iPod was launched in 2001, which marked the company's first venture away from computers and into other segments of consumer electronics. With several hundred million units sold, the iPod was a tremendous success. Its popularity however started to decline in 2008, as advanced music functions of smartphones began to substitute MP3 players. Apple's digital media store, the iTunes Store, was launched in 2003 and became one of the most popular online music stores in the world, generating several billion U.S. dollars in revenue per quarter.

In 2007, the release of the iPhone marked a revolution for the global smartphone market, due to the introduction of the first touch screen interface. In the United States especially, the iPhone has been a key product for the company, generating millions of unit sales and high levels of revenue. The iPhone is currently contributing about 60 percent to the company's total revenue. In total, Apple has sold close to 1.5 billion iPhones from 2007 to 2018 worldwide.

In January 2010, the iPad was unveiled, marking yet another milestone in the industry. The device went on to sell more than 3 million units in the first 3 months, thus setting a new benchmark in the industry. With the launch of its Apple Watch in early 2015, Apple entered the growing wearables market, competing with companies such as Samsung, Pebble and Fitbit.

As of June 2018, Apple's market capitalization reached 950 billion U.S. dollars, higher than that of competitors such as Microsoft, IBM and Google, and almost ten times more than its own capitalization in 2006. The company's market cap topped the one trillion U.S. dollars mark on 2. August, 2018, becoming the first public company worldwide to reach that milestone. After hitting a record high of 1.12 trillion in October 2018, Apple's market cap slowly dropped back to the sub-trillion level.

Apple updated its U.S. job creation web page with figures from 2016. Though Apple refreshes the site every year, this latest update coincides with CEO Tim Cook's

announcement during a CNBC interview that the company has formed a $1 billion fund to promote advanced manufacturing jobs in the U.S.

Though the fund may help the company gain favor with the current presidential administration, Apple has already been investing in U.S. hardware manufacturing for years (for example, its 2013 Mac Pros were built in Texas with U.S.-made components).

In total, Apple says it has created a total of two million jobs in the U.S. so far. In 2015 Apple spent more than $50 billion with 9,000 U.S. suppliers and manufacturers and added about 90,000 supplier and manufacturer jobs, increasing the total number to 450,000 jobs from 361,000 in 2015.

The number of people directly employed by Apple, including at its retail stores, grew from 76,000 to 80,000 in 2016.

On the software side, Apple claims that 1,530,000 U.S. jobs can be attributed to the App Store ecosystem, up from 1,400,000 in 2015. Since the App Store was launched in 2008, U.S. developers have earned $16 billion from sales, with 39 percent of that amount generated from abroad.

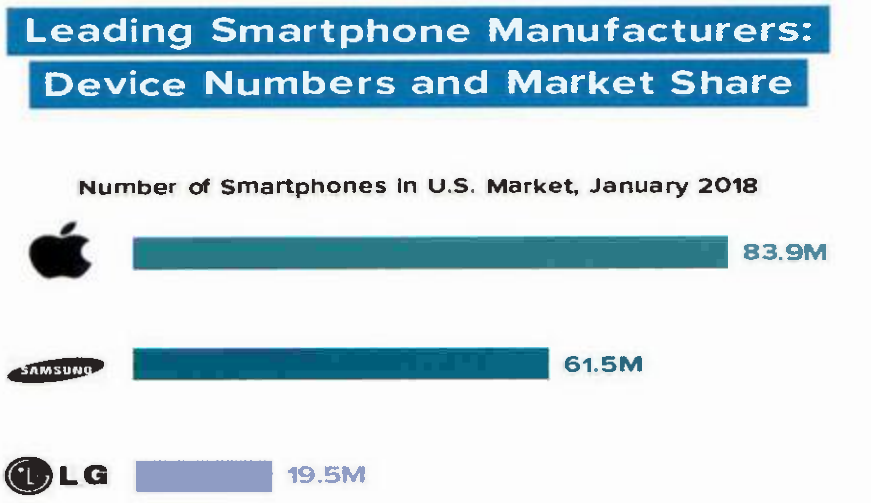
Apple also said that all of its main products (the iPhone, iPad, Mac, Apple Watch, and Apple TV) contain materials from the U.S. or are made with equipment from U.S. suppliers). It has reportedly asked its main manufacturing partners, including Foxconn, to open more factories in the U.S.

During the CNBC interview, Cook told Jim Cramer that the company will hire "thousands of employees" and is "not satisfied with just two million."

"By doing that, we can be the ripple in the pond," Cook said. "Because if we can create many manufacturing jobs around–those manufacturing jobs create more jobs around them, because you have a service industry that builds up around them."

Reference: This text provides general information. Statista assumes no liability for the information given being complete or correct. Due to varying update cycles, statistics can display more up-to-date data than referenced in the text. Image Credits: bennymarty (opens in a new window)/ Getty Images

How Do Apple, Samsung, and LG Stack Up?



Verto Analytics looked at the numbers of Apple, Samsung, and LG smartphones currently owned by U.S. consumers, and the equivalent market share. January 2018, Apple leads the pack, with 45% market share (representing nearly 84 million smartphones), while Samsung claims 33% of the market (61.5 million smartphones). These two manufacturers dominate the U.S. smartphone market; LG, the third-place contender, has 10% market share, while all other brands combined account for 12% of the devices on the U.S. smartphone market.

This Chart of the Week was created using Verto Watch.

LARRY GOLDEN
740 WOODRUFF RD. #1102
GREENVILLE, SC 29607

Retail

UNITED STATES POSTAL SERVICE

20439

RDC 07

U.S. POSTAGE PAID
PME
GREENVILLE, SC 29616
JAN 18, 2025

$43.90

S2324K504193-25

UNITED STATES POSTAL SERVICE®

PRIORITY MAIL EXPRESS®

EI 935 866 458 US

CUSTOMER USE ONLY

FROM: (PLEASE PRINT) PHONE 864 992-7104

LARRY GOLDEN
740 WOODRUFF RD.
#1102
GREENVILLE, SC 29607

DELIVERY OPTIONS (Customer Use Only)

SIGNATURE REQUIRED Note: The mailer must check the "Signature Required" box if the mailer: 1) Requires the addressee's signature; OR 2) Purchases additional insurance; OR 3) Purchases COD service; OR 4) Purchases Return Receipt service. If the box is not checked, the Postal Service will leave the item in the addressee's mail receptacle or other secure location without attempting to obtain the addressee's signature on delivery.

Delivery Options
- ☐ No Saturday Delivery (delivered next business day)
- ☐ Sunday/Holiday Delivery Required (additional fee, where available*)
  *Refer to USPS.com® or local Post Office™ for availability.

TO: (PLEASE PRINT) PHONE 202 275-8000

U.S. COURT OF APPEALS FOR THE FEDERAL CIRCUIT
CASE NO: 24-2256
717 MADISON PLACE, N.W.
WASHINGTON, D.C.
ZIP + 4® (U.S. ADDRESSES ONLY)
20439-____

- For pickup or USPS Tracking™, visit USPS.com or call 800-222-1811.
- $100.00 insurance included.

PEEL FROM THIS CORNER

PAYMENT BY ACCOUNT (if applicable)
Federal Agency Acct. No. or Postal Service™ Acct. No.

ORIGIN (POSTAL SERVICE USE ONLY)

☐ 1-Day ☑ 2-Day ☐ Military ☐ DPO

PO ZIP Code	Scheduled Delivery Date (MM/DD/YY)	Postage
29616	1/21/25	$ 43.90

Date Accepted (MM/DD/YY)	Scheduled Delivery Time	Insurance Fee	COD Fee
1/18/25	☐ 6:00 PM 6pm	$	$

Time Accepted		Return Receipt Fee	Live Animal Transportation Fee
10:28	☑ AM ☐ PM	$	$

Special Handling/Fragile	Sunday/Holiday Premium Fee	Total Postage & Fees
$	$	$ 43.90

Weight: 13.90 lbs. ozs. ☐ Flat Rate | Acceptance Employee Initials:

DELIVERY (POSTAL SERVICE USE ONLY)

Delivery Attempt (MM/DD/YY)	Time	Employee Signature
	☐ AM ☐ PM	
Delivery Attempt (MM/DD/YY)	Time	Employee Signature
	☐ AM ☐ PM	

LABEL 11-B, NOVEMBER 2023 PSN 7690-02-000-9996